



Industrie des cartes de paiement (PCI) Norme de sécurité des données

Conditions et procédures d'évaluation de sécurité

Version 3.2
Avril 2016

Modifications apportées au document

Date	Version	Description	Pages
Octobre 2008	1.2	Afin de présenter la v1.2 de la norme PCI DSS comme les « Conditions et procédures d'évaluation de sécurité PCI DSS », élimination des redondances entre les documents et changements d'ordre général et spécifique par rapport à la v1.1 des Procédures d'audit de sécurité PCI DSS. Pour des informations complètes, consulter le document PCI Norme de sécurité des données – Récapitulatif des modifications entre les versions 1.1 et 1.2. de la norme PCI DSS.	
Juillet 2009	1.2.1	Ajout d'une phrase supprimée par erreur entre les v1.1 et v1.2 de la norme PCI DSS.	5
		Correction de « ensuite » par « que » dans les procédures de test 6.3.7.a et 6.3.7.b.	32
		Suppression des marques grisées des colonnes « En place » et « Pas en place » dans la procédure de test 6.5.b.	33
		Pour le document Fiche de contrôles compensatoires – Exemple complété, correction de vocabulaire en haut de page pour dire « Se référer à cette fiche pour définir des contrôles compensatoires pour toute condition indiquée comme « en place » par le biais des contrôles compensatoires. »	64
Octobre 2010	2.0	Mise à jour et application des changements depuis la v1.2.1. Voir <i>PCI DSS – Récapitulatif des modifications entre les versions 1.2.1 et 2.0 de la norme PCI DSS</i>	
Novembre 2013	3.0	Mise à jour de la v2.0. Voir <i>PCI DSS – Récapitulatif des modifications entre les versions 2.0 et 3.0 de la norme PCI DSS</i>	
Avril 2015	3.1	Mise à jour de la norme PCI DSS v3.0. Pour plus de détails sur les modifications, veuillez consulter <i>PCI DSS – Récapitulatif des modifications entre les versions 3.0 et 3.1 de la norme PCI DSS</i> .	
Avril 2016	3.2	Mise à jour de la norme PCI DSS v3.1. Pour plus de détails sur les modifications, veuillez consulter <i>PCI DSS – Récapitulatif des modifications entre les versions 3.1 et 3.2 de la norme PCI DSS</i> .	

Table des matières

Avril 2016	2
Modifications apportées au document	2
Introduction et présentation de la norme de sécurité des données PCI	5
<i>Ressources de la norme PCI DSS.....</i>	<i>6</i>
Informations relatives aux conditions d'application de la norme PCI DSS.....	7
Relation entre les normes PCI DSS et PA-DSS.....	9
<i>Conditions d'application de la norme PCI DSS aux applications PA-DSS</i>	<i>9</i>
<i>Conditions d'application de la norme PCI DSS aux fournisseurs d'application de paiement.....</i>	<i>9</i>
Champ d'application des conditions de la norme PCI DSS.....	10
<i>Segmentation réseau</i>	<i>11</i>
<i>Technologie sans-fil.....</i>	<i>12</i>
<i>Utilisation de prestataires de services tiers/sous-traitance</i>	<i>12</i>
Meilleures pratiques d'implémentation de la norme PCI DSS dans les processus d'affaires courantes	14
Pour les évaluateurs : Échantillonnage des installations de l'entreprise et des composants de système	16
Contrôles compensatoires.....	17
Instructions et contenu du Rapport sur la conformité	18
Processus d'évaluation de la norme PCI DSS.....	18
Versions de PCI DSS.....	19
Conditions et procédures d'évaluation de sécurité détaillées de la norme PCI DSS.....	20
Création et gestion d'un réseau et d'un système sécurisés.....	21
<i>Condition 1 : Installer et gérer une configuration de pare-feu pour protéger les données de titulaires de carte</i>	<i>21</i>
<i>Condition 2 : Ne pas utiliser les mots de passe système et autres paramètres de sécurité par défaut définis par le fournisseur</i>	<i>30</i>
Protection des données de titulaires de carte.....	38
<i>Condition 3 : Protéger les données de titulaires de carte stockées.....</i>	<i>38</i>
<i>Condition 4 : Crypter la transmission des données de titulaires de carte sur les réseaux publics ouverts</i>	<i>53</i>
Gestion d'un programme de gestion des vulnérabilités	56
<i>Condition 5 : Protéger tous les systèmes contre les logiciels malveillants et mettre à jour régulièrement les logiciels anti-virus ou programmes w</i>	<i>56</i>
<i>Condition 6 : Développer et maintenir des systèmes et des applications sécurisés.....</i>	<i>60</i>

Mise en œuvre de mesures de contrôle d'accès strictes.....	76
<i>Condition 7 : Restreindre l'accès aux données de titulaires de carte aux seuls individus qui doivent les connaître</i>	<i>76</i>
<i>Condition 8 : Identifier et authentifier l'accès aux composants de système.....</i>	<i>79</i>
<i>Condition 9 : Restreindre l'accès physique aux données de titulaires de carte.....</i>	<i>92</i>
Surveillance et test réguliers des réseaux.....	105
<i>Condition 10 : Effectuer le suivi et surveiller tous les accès aux ressources réseau et aux données de titulaires de carte</i>	<i>105</i>
<i>Condition 11 : Tester régulièrement les processus et les systèmes de sécurité</i>	<i>115</i>
Gestion d'une politique de sécurité des informations.....	126
<i>Condition 12 : Maintenir une politique qui adresse les informations de sécurité pour l'ensemble du personnel.....</i>	<i>126</i>
Annexe A : Autres conditions de la norme PCI DSS	139
<i>Annexe A1 : Autres conditions de la norme PCI DSS s'appliquant aux fournisseurs d'hébergement partagé.....</i>	<i>140</i>
<i>Annexe A2 : Autres conditions de la norme PCI DSS s'appliquant aux entités qui utilisent le SSL/TLS initial</i>	<i>142</i>
<i>Annexe A3 : Validation complémentaire des entités désignées (DESV).....</i>	<i>146</i>
Annexe B : Contrôles compensatoires.....	164
Annexe C : Fiche de contrôles compensatoires.....	166
Annexe D : Segmentation et échantillonnage des installations de l'entreprise et des composants de système.....	169

Introduction et présentation de la norme de sécurité des données PCI

La Norme de sécurité des données de l'industrie des cartes de paiement (PCI DSS) a été développée dans le but d'encourager et de renforcer la sécurité des données de titulaires de carte ainsi que pour faciliter l'adoption de mesures de sécurité uniformes à l'échelle mondiale. La norme PCI DSS sert de référence aux conditions techniques et opérationnelles conçues pour protéger les données de compte. La norme PCI DSS s'applique à **toutes** les entités impliquées dans le traitement des cartes de paiement, notamment les commerçants, les entreprises de traitement, les acquéreurs, les émetteurs et les prestataires de services. La norme PCI DSS s'applique également à **toutes** les autres entités qui stockent, traitent ou transmettent les données de titulaires de cartes (cardholder data, CHD) et/ou les données d'identification sensibles (sensitive authentication data, SAD). Les 12 clauses de la norme PCI DSS sont détaillées ci-dessous.

PCI DSS – Présentation détaillée

Création et gestion d'un réseau et d'un système sécurisés	<ol style="list-style-type: none"> 1. Installer et gérer une configuration de pare-feu pour protéger les données de titulaires de carte 2. Ne pas utiliser les mots de passe système et autres paramètres de sécurité par défaut définis par le fournisseur
Protection des données de titulaires de carte	<ol style="list-style-type: none"> 3. Protéger les données de titulaires de carte stockées 4. Crypter la transmission des données de titulaires de carte sur les réseaux publics ouverts
Gestion d'un programme de gestion des vulnérabilités	<ol style="list-style-type: none"> 5. Protéger tous les systèmes contre les logiciels malveillants et mettre à jour régulièrement les logiciels ou programmes anti-virus 6. Développer et maintenir des systèmes et des applications sécurisés
Mise en œuvre de mesures de contrôle d'accès strictes	<ol style="list-style-type: none"> 7. Restreindre l'accès aux données de titulaires de carte aux seuls individus qui doivent les connaître 8. Identifier et authentifier l'accès à tous les composants de système 9. Restreindre l'accès physique aux données de titulaires de carte
Surveillance et test réguliers des réseaux	<ol style="list-style-type: none"> 10. Effectuer le suivi et surveiller tous les accès aux ressources réseau et aux données de titulaires de carte 11. Tester régulièrement les processus et les systèmes de sécurité
Gestion d'une politique de sécurité des informations	<ol style="list-style-type: none"> 12. Gérer une politique de sécurité des informations pour l'ensemble du personnel

Le présent document, intitulé *Conditions et procédures d'évaluation de sécurité de la norme PCI DSS*, combine les 12 conditions de la norme PCI DSS et les procédures de test correspondantes en un outil d'évaluation de sécurité. Il est conçu pour être utilisé au cours des évaluations de conformité PCI DSS, dans le cadre du processus de validation d'une entité. Les sections suivantes détaillent les directives et meilleures pratiques

afin d'aider les entités à se préparer à une évaluation PCI DSS, à la mener à bien et à en rapporter les résultats. Les conditions de la norme PCI DSS et les procédures de test commencent en page 15

La norme PCI DSS comprend un ensemble de conditions pour la protection des données de compte et peut être renforcée de contrôles et de pratiques supplémentaires pour atténuer encore les risques, ainsi que par des lois et réglementations locales, régionales et sectorielles. En outre, les conditions législatives ou réglementaires peuvent exiger une protection spécifique des informations personnelles ou autres éléments de données (par exemple, le nom du titulaire de carte). La norme PCI DSS ne supprime pas les lois locales ou régionales, les réglementations gouvernementales ou autres obligations légales.

Ressources de la norme PCI DSS

Le site Web du Conseil des normes de sécurité PCI (PCI SSC) (www.pcisecuritystandards.org) contient plusieurs ressources supplémentaires, destinées à aider les organisations au cours des validations et évaluations de la norme PCI DSS, y compris :

- Une bibliothèque de documents comprenant :
 - *PCI DSS – Récapitulatif des modifications entre les versions 2.0 et 3.0 de la norme PCI DSS*
 - *Guide de référence rapide de la norme PCI DSS*
 - *Glossaire des termes, abréviations et acronymes PCI DSS et PA-DSS*
 - *Suppléments d'information et directives*
 - *Approche prioritaire pour la norme PCI DSS*
 - *Rapport sur la conformité (ROC) Modèle de rapport et instructions concernant le rapport*
 - *Questionnaires d'auto-évaluation (SAQ), instructions et directives relatives au SAQ*
 - *Attestations de conformité (AOC)*
- Questions fréquentes (FAQ)
- PCI pour les sites Web de commerçants de petite taille
- Cours de formation PCI et webinaires d'information
- Liste des évaluateurs de sécurité qualifiée (Qualified Security Assessors, QSA) et des prestataires de services d'analyse (Approved Scanning Vendors, ASV)
- Liste des appareils approuvés par PTS et des applications de paiement validées selon la norme PA-DSS

Remarque : Les suppléments d'information complètent la norme PCI DSS et identifient des considérations et recommandations supplémentaires pour remplir les conditions de la norme PCI DSS —Elles ne supplantent pas, ne remplacent pas et ne développent pas la norme PCI DSS, ni aucune de ses conditions.

Veuillez consulter www.pcisecuritystandards.org pour de plus amples informations concernant ces ressources et d'autres ressources.

Informations relatives aux conditions d'application de la norme PCI DSS

La norme PCI DSS s'applique à **toutes** les entités impliquées dans le traitement des cartes de paiement, notamment les commerçants, les entreprises de traitement, les acquéreurs, les émetteurs et les prestataires de services. La norme PCI DSS s'applique également à **toutes** les autres entités qui stockent, traitent ou transmettent les données de titulaires de carte et/ou les données d'identification sensibles.

Les données de titulaires de carte et les données d'identification sensibles sont définies comme suit :

Données de compte	
Les données de titulaires de carte comprennent :	Les données d'identification sensibles comprennent :
<ul style="list-style-type: none"> ▪ Numéro de compte primaire (PAN) ▪ Nom du titulaire de la carte ▪ Date d'expiration ▪ Code service 	<ul style="list-style-type: none"> ▪ Données de bande magnétique complètes (données de bande magnétique ou équivalent sur une puce) ▪ CAV2/CVC2/CVV2/CID ▪ Codes/blocs PIN

Le numéro de compte primaire est le facteur de définition des données de titulaires de carte. Si le nom du titulaire de carte, le code service et/ou la date d'expiration sont stockés, traités ou transmis avec le PAN, ou existent d'une façon ou d'une autre dans l'environnement des données de titulaires de carte (cardholder data environment, CDE), ils doivent être protégés conformément à toutes les conditions applicables de la norme PCI DSS.

Les conditions de la norme PCI DSS s'appliquent aux organisations où les données de compte (données de titulaires de carte et/ou données d'identification sensibles) sont stockées, traitées ou transmises. Certaines conditions de la norme PCI DSS peuvent aussi s'appliquer aux organisations qui ont sous-traité les opérations de paiement ou la gestion de leur CDE¹. De plus, les organisations qui sous-traitent leur CDE ou leurs opérations de paiement à des tiers doivent s'assurer que les données de comptes sont protégées par le tiers, conformément aux conditions applicables de la norme PCI DSS.

Le tableau de la page suivante présente un certain nombre d'éléments courants des données de titulaires de carte et des données d'identification sensibles, indique si le stockage de chaque élément de données est autorisé ou interdit, et précise si chaque élément de données doit être protégé. Ce tableau n'est pas exhaustif, mais il est présenté de manière à illustrer les différents types de conditions qui s'appliquent à chaque élément de données.

¹ Selon les programmes de conformité des marques de paiement individuelles

		Élément de données	Stockage autorisé	Rendre illisibles les données stockées selon la condition 3.4
Données de compte	Données de titulaires de carte	Numéro de compte primaire (PAN)	Oui	Oui
		Nom du titulaire de la carte	Oui	Non
		Code service	Oui	Non
		Date d'expiration	Oui	Non
	Données d'identification sensibles ²	Données complètes de piste magnétique ³	Non	Stockage interdit selon la condition 3.2
		CAV2/CVC2/CVV2/CID ⁴	Non	Stockage interdit selon la condition 3.2
		Code/bloc PIN ⁵	Non	Stockage interdit selon la condition 3.2

Les conditions 3.3 et 3.4 de la norme PCI DSS ne s'appliquent qu'au PAN. Si le PAN est stocké avec d'autres données de titulaires de carte, seul le PAN doit être rendu illisible selon la condition 3.4 de la norme PCI DSS.

Les données d'identification sensibles ne doivent pas être stockées après autorisation, même si elles sont cryptées. Cela s'applique même lorsqu'il n'y a pas de PAN dans l'environnement. Les organisations doivent contacter directement leur acquéreur ou la marque de paiement individuelle afin de savoir s'il est permis de stocker un SAD avant autorisation, pendant combien de temps, ainsi que pour connaître toute condition d'utilisation et de protection en rapport.

² Une fois le processus d'autorisation terminé, les données d'identification sensibles ne peuvent plus être stockées (même si elles sont cryptées).

³ Données de piste complètes extraites de la bande magnétique, données équivalentes sur la puce, ou autre support

⁴ Le nombre à trois ou quatre chiffres figurant au recto ou au verso de la carte de paiement

⁵ Le numéro d'identification personnel saisi par le titulaire de la carte lors d'une transaction carte présente et/ou le bloc PIN crypté présent dans le message de la transaction

Relation entre les normes PCI DSS et PA-DSS

Conditions d'application de la norme PCI DSS aux applications PA-DSS

L'utilisation seule d'une application conforme à la norme Payment Application Norme de sécurité des données (PA-DSS), n'en fait pas une entité conforme à la norme PCI DSS, car elle doit être mise en œuvre dans un environnement respectant ces normes, conformément au Guide de mise en œuvre de la norme PA-DSS remis par le fournisseur d'applications de paiement.

Toutes les applications qui stockent, traitent ou transmettent les données de titulaires de carte peuvent faire l'objet d'une évaluation PCI DSS d'une entité, y compris les applications qui ont été validées pour PA-DSS. L'évaluation PCI DSS doit vérifier que l'application de paiement validée PA-DSS est correctement configurée et implémentée de manière sécuritaire selon les exigences de la norme PCI DSS. Si l'application de paiement a donné lieu à une personnalisation, un examen plus approfondi sera requis pendant l'évaluation PCI DSS, dans la mesure où l'application est susceptible de ne plus être représentative de la version validée PA-DSS.

Les conditions de la norme PA-DSS sont issues des *Conditions et procédures d'évaluation de sécurité de la norme PCI DSS* (définies dans le présent document). La norme PA-DSS détaille ce qu'une application de paiement doit prendre en charge pour permettre la conformité d'un client à la norme PCI DSS. Dans la mesure où les menaces de sécurité sont en constante évolution, les applications qui ne sont plus prises en charge par le fournisseur (par exemple identifiées par le fournisseur comme étant en fin de vie) sont susceptibles de ne pas offrir le même niveau de sécurité que les versions prises en charge.

Les applications de paiement sécurisées, lorsqu'elles sont mises en œuvre dans un environnement conforme à la norme PCI DSS, réduisent le risque que des failles de sécurité compromettant les données de PAN, les données complètes de piste, les codes et valeurs de validation de carte (CAV2, CID, CVC2, CVV2), les codes et les blocs PIN, ainsi que la fraude nuisible résultant de ces failles.

Pour déterminer si la norme PA-DSS s'applique à une application de paiement donnée, veuillez consulter le Guide du programme de la norme PA-DSS, disponible sur www.pcisecuritystandards.org.

Conditions d'application de la norme PCI DSS aux fournisseurs d'application de paiement.

La norme PCI DSS est susceptible de s'appliquer aux fournisseurs d'application de paiement si le fournisseur stocke, traite ou transmet des données de titulaires de carte, ou a accès aux données de titulaires de carte de ses clients (par exemple, dans le rôle d'un fournisseur de services).

Champ d'application des conditions de la norme PCI DSS

Les conditions de sécurité de la norme PCI DSS, s'appliquent à tous les composants de système inclus ou connectés à l'environnement des données de titulaires de carte. L'environnement des données de titulaires de carte (CDE) est constitué d'individus, de processus et de technologies qui stockent, traitent, ou transmettent les données de titulaires de carte ou les données d'identification sensibles. Les « composants de système » comprennent les dispositifs de réseau, les serveurs, les périphériques informatiques et les applications. Les exemples de composants de système comprennent notamment :

- Les systèmes qui fournissent des services de sécurité (par exemple, les serveurs d'authentification), facilitent la segmentation (par exemple, les pare-feu internes) ou qui pourraient avoir un impact sur le CDE (par exemple, des serveurs de résolution de nom ou de redirection Web).
- Les composants de virtualisation comme les machines virtuelles, commutateurs/routeurs virtuels, outils virtuels, applications/bureaux virtuels ainsi que les hyperviseurs.
- Les composants réseau comprennent notamment les pare-feu, les commutateurs, les routeurs, les points d'accès sans-fil, les équipements réseau et autres appareils de sécurité.
- Les types de serveur comprennent notamment les serveurs Web, d'application, de base de données, d'authentification, de messagerie, proxy, NTP (Network Time Protocol - Protocole d'Heure Réseau) et DNS (Domain Name System - Système de Noms de Domaine).
- Les applications comprennent toutes les applications achetées et personnalisées, y compris les applications internes et externes (par exemple Internet).
- Tout autre composant ou dispositif situé à l'intérieur du CDE ou connecté au CDE.

La première étape d'une évaluation PCI DSS est de correctement déterminer le champ d'application de la vérification. Au moins une fois par an, et avant l'évaluation annuelle, l'entité évaluée doit confirmer l'exactitude de son champ d'application de la norme PCI DSS en identifiant tous les emplacements et flux des données de titulaires de carte et s'assurer que tous les systèmes qui y sont connectés, ou en cas d'incident de sécurité, peuvent se connecter au CDE (par exemple, les serveurs d'authentification) pour veiller à les inclure dans le champ d'application de la norme PCI DSS. Tous les types de systèmes et d'emplacements doivent être pris en compte dans le processus de la détermination du champ d'application, y compris les sites de sauvegarde/rétablissement et les systèmes de reprise des services.

Pour confirmer l'exactitude du CDE défini, procéder comme suit :

- L'entité évaluée identifie et documente l'existence de toutes les données de titulaires de carte dans son environnement, afin de vérifier qu'aucune donnée n'existe en dehors du CDE actuellement défini.
- Une fois tous les emplacements de données de titulaires de carte identifiés et documentés, l'entreprise utilise les résultats pour vérifier que le champ d'application PCI DSS est approprié (par exemple, les résultats peuvent être un diagramme ou un inventaire des emplacements des données de titulaires de carte).

- L'entité considère que toutes données de titulaires de carte trouvées s'inscrivent dans le cadre de l'évaluation PCI DSS et fait partie du CDE. Si l'entité identifie des données qui ne sont pas actuellement incluses dans le CDE, ces données doivent être supprimées de manière sécuritaire, déplacées vers le CDE actuellement défini ou le CDE redéfini doit inclure ces données.

L'entité conserve la documentation qui montre comment la portée de la norme PCI DSS a été déterminée. La documentation est conservée pour l'examen de l'évaluateur et/ou pour référence au cours de l'activité annuelle de confirmation du champ d'application de la norme PCI DSS.

Pour chaque évaluation PCI DSS, l'évaluateur doit valider que la portée de l'évaluation soit effectivement définie et documentée.

Segmentation réseau

La segmentation réseau, ou l'isolation (segmentation), de l'environnement des données de titulaires de carte par rapport au reste du réseau de l'entreprise n'est pas une condition de la norme PCI DSS. Toutefois, cette approche est vivement recommandée dans la mesure où elle contribue à réduire :

- le champ d'application de l'évaluation PCI DSS ;
- les coûts de l'évaluation PCI DSS ;
- les coûts et les difficultés liés à la mise en œuvre et à la gestion des contrôles PCI DSS ;
- les risques pour une entreprise (réduits grâce au regroupement des données de titulaires de carte dans un nombre plus restreint de sites mieux contrôlés).

Sans une segmentation réseau adéquate (parfois appelée « réseau plat »), l'ensemble du réseau est inclus dans le champ d'application de l'évaluation PCI DSS. La segmentation réseau peut être réalisée par le biais d'un certain nombre de moyens physiques ou logiques, pare-feu réseau internes correctement configurés et routeurs associés à des listes de contrôle d'accès strictes ou autres technologies qui restreignent l'accès à un segment particulier du réseau. Pour être considéré comme étant hors champ d'application de la norme PCI DSS, un composant de système doit être isolé (segmenté) correctement du CDE, de telle sorte que, même si le composant hors champ d'application devait être compromis, la sécurité du CDE ne serait pas mise en péril.

Pour limiter le champ d'application de l'environnement des données de titulaires de carte, il est important d'identifier clairement les besoins de l'entreprise et les processus liés au stockage, au traitement ou à la transmission des données de titulaires de carte. Le regroupement des données de titulaires de carte dans un nombre d'emplacements aussi restreint que possible, en éliminant les données superflues et en consolidant les données nécessaires, peut impliquer la refonte des pratiques commerciales traditionnelles.

La documentation des flux de données de titulaires de carte par le biais d'un schéma de flux des données permet de comprendre parfaitement tous les flux de données de titulaires de carte et de s'assurer que toute segmentation réseau isole correctement l'environnement des données de titulaires de carte.

Si une segmentation réseau est en place et doit servir à réduire le champ d'application de l'évaluation PCI DSS, l'évaluateur doit s'assurer qu'elle convient bien à cette fin. À un niveau supérieur, la segmentation réseau isole les systèmes qui stockent, traitent ou transmettent les données de titulaires de carte des autres systèmes. Toutefois, l'adéquation d'une implémentation spécifique de la segmentation réseau peut

varier considérablement et dépend de facteurs tels que la configuration d'un réseau, les technologies déployées et d'autres contrôles susceptibles d'être mis en œuvre.

Annexe D : La segmentation et l'échantillonnage des installations de l'entreprise et des composants de système fournissent de plus amples informations sur l'effet de la segmentation réseau et de l'échantillonnage sur le champ d'application de l'évaluation PCI DSS.

Technologie sans-fil

Si une technologie sans-fil est utilisée pour stocker, traiter ou transmettre les données de titulaires de carte (par exemple, transactions des points de vente et « line busting » [ou élimination des files d'attente aux points de paiement]), ou si un réseau local (WLAN) sans-fil est connecté à l'environnement des données de titulaires de carte ou en fait partie, les conditions de la norme PCI DSS et les procédures de test pour les environnements sans-fil s'appliquent et doivent être exécutées (par exemple, conditions 1.2.3, 2.1.1 et 4.1.1). Avant de mettre en œuvre la technologie sans-fil, une entreprise doit soigneusement évaluer la nécessité de déployer cette technologie par rapport aux risques induits. Le déploiement de la technologie sans-fil ne doit être envisagé que pour la transmission de données non sensibles.

Utilisation de prestataires de services tiers/sous-traitance

Un prestataire de services ou un commerçant peuvent faire appel à un prestataire tiers pour le stockage, le traitement ou la transmission des données de titulaires de carte en son nom, ou pour la gestion de composants tels que les routeurs, les pare-feu, les bases de données, la sécurité physique et/ou les serveurs. Dans ce cas, la sécurité de l'environnement des données de titulaires de carte peut s'en trouver affectée.

Les parties doivent clairement identifier les services et les composants de système qui sont inclus dans la portée de l'évaluation PCI DSS du prestataire de service, les conditions spécifiques de la norme PCI DSS couvertes par le prestataire de service, ainsi que toutes les conditions pour lesquelles les clients du prestataire de services doivent inclure leurs propres examens PCI DSS. Par exemple, un fournisseur d'hébergement géré doit clairement définir quelles sont ses adresses IP qui sont analysées dans le cadre de leur processus trimestriel d'analyse de vulnérabilité, ainsi que les adresses IP que le client doit inclure dans ses propres analyses trimestrielles.

Il incombe aux prestataires de services de prouver la conformité à la norme PCI DSS. Ils seront peut-être amenés à le faire par des marques de paiement. Les prestataires de services doivent contacter leur acquéreur et/ou marque de paiement pour déterminer la validation de conformité appropriée.

Il existe deux options de validation de la conformité des prestataires de services tiers :

- 1) **Évaluation annuelle** : Les prestataires de services peuvent faire l'objet d'une ou de plusieurs évaluations annuelles de la norme PCI DSS de leur propre chef et fournir à leurs clients la preuve de leur conformité ; ou
- 2) **Plusieurs évaluations, à la demande** : S'ils n'effectuent pas leurs propres évaluations annuelles de la norme PCI DSS, les prestataires de services doivent réaliser des évaluations à la demande de leurs clients et/ou participer à chacun des examens PCI DSS de leurs clients sachant que les résultats de chaque examen sont soumis au ou aux clients concernés

Si le tiers effectue sa propre évaluation PCI DSS, il doit fournir suffisamment de preuves à ses clients pour vérifier que la portée de l'évaluation PCI DSS du prestataire a recouvert les services applicables au client et que les conditions pertinentes de la norme PCI DSS ont été examinées et déterminées comme ayant été mises en place. Le type de preuve spécifique fourni par le prestataire de service à ses clients dépendra de

l'accord/contrat passé entre ces parties. Par exemple, si l'AOC et/ou les sections pertinentes de l'AOC du prestataire de service (rédigées de manière à protéger toute information confidentielle) pourraient aider à trouver tout ou partie de l'information.

En outre, les commerçants et les prestataires de services doivent gérer et contrôler la conformité à la norme PCI DSS de tous les prestataires tiers qui ont accès aux données de titulaires de carte auxquels ils sont associés. *Pour plus d'informations, se reporter à la condition 12.8 du présent document.*

Meilleures pratiques d'implémentation de la norme PCI DSS dans les processus d'affaires courantes

Pour assurer que les contrôles de sécurité continuent d'être correctement mis en œuvre, la norme PCI DSS doit être implémentée dans les activités d'affaires courantes (BAU) dans le cadre de la stratégie de sécurité globale de l'entité. Cette pratique permet à une entité de surveiller l'efficacité de leurs contrôles de sécurité sur une base continue et de maintenir la conformité de leur environnement à la norme PCI DSS entre les évaluations PCI DSS. Les exemples du mode d'insertion de la norme PCI DSS aux activités BAU comprennent, mais sans s'y limiter, ce qui suit :

1. La surveillance des contrôles de sécurité, tels que les pare-feu, les systèmes de détection d'intrusion/systèmes de prévention des intrusions (IDS/IPS), la surveillance d'intégrité de fichier (FIM), les anti-virus, les contrôles d'accès, etc. ; pour garantir qu'ils fonctionnent de manière efficace comme prévu.
2. Assurer que les défaillances des contrôles de sécurité soient détectées et résolues rapidement Les processus de résolution des défaillances des contrôles de sécurité doivent comprendre :
 - La restauration des contrôles de sécurité ;
 - L'identification des causes de la défaillance ;
 - L'identification et la résolution des problèmes de sécurité survenus pendant la défaillance du contrôle de sécurité ;
 - L'implémentation des mesures d'atténuation (telles que les processus et les contrôles techniques) pour empêcher que la cause de la défaillance ne se reproduise ;
 - La reprise de la surveillance des contrôles de sécurité, éventuellement avec une surveillance accrue pendant un certain temps, afin de vérifier que le contrôle fonctionne de manière efficace.
3. Examiner les modifications de l'environnement (par exemple, l'ajout de nouveaux systèmes, les changements de configurations de système ou de réseau) avant la fin des modifications et effectuer les procédures suivantes :
 - Déterminer l'impact potentiel sur la portée de la norme PCI DSS (par exemple, une nouvelle règle de pare-feu qui permet la connectivité entre un système du CDE et un autre système pourrait amener des systèmes ou des réseaux supplémentaires dans la portée de la norme PCI DSS).
 - Identifier les conditions de la norme PCI DSS applicables aux systèmes et aux réseaux affectés par les changements (par exemple, si un nouveau système se trouve dans le champ d'application de la norme PCI DSS, il doit être configuré selon les normes de configuration de système, en tenant compte de la FIM, AV, des correctifs, de la journalisation d'audit, etc. ; et il doit être ajouté au programme d'analyse de vulnérabilité trimestriel).
 - Mettre à jour le champ d'application de la norme PCI DSS et implémenter les contrôles de sécurité de manière appropriée.
4. Les changements de la structure organisationnelle (par exemple l'intégration ou l'acquisition d'une société) se soldent par un examen formel de l'impact sur le champ d'application et les conditions de la norme PCI DSS.

5. Des examens et des communications périodiques doivent être effectués pour confirmer que les conditions de la norme PCI DSS demeurent en place et que le personnel respecte les processus de sécurité. Ces examens périodiques doivent recouvrir toutes les installations et tous les emplacements, y compris les détaillants, les centres de données, etc., et inclure un examen de tous les composants de système (ou des échantillons de composants de système), pour vérifier que les conditions de la norme PCI DSS demeurent en place, par exemple, les standards de configuration ont été appliqués, les correctifs et AV sont à jour, les journaux d'audit sont analysés et ainsi de suite. La fréquence des examens périodiques doit être déterminée par l'entité en fonction de la taille et de la complexité de son environnement.

Les examens peuvent également être utilisés pour vérifier que les preuves suffisantes sont maintenues, par exemple journaux d'audit, rapports d'analyse de vulnérabilité, examens de pare-feu, etc. afin d'aider l'entité à se préparer pour sa prochaine évaluation de conformité.

6. Examiner les technologies matérielles et logicielles au moins une fois par an pour confirmer qu'elles continuent à être prises en charge par le fournisseur et qu'elles respectent les conditions de sécurité de l'entité, y compris celles de la norme PCI DSS. S'il s'avère que les technologies ne sont plus prises en charge par le fournisseur ou qu'elles ne peuvent plus répondre aux besoins de sécurité de l'entité, celle-ci doit préparer un plan de réparation, qui peut comprendre le remplacement de la technologie si besoin.

En plus des pratiques ci-dessus, les organisations peuvent également envisager la séparation des tâches pour leurs fonctions de sécurité de sorte que les fonctions de sécurité et/ou d'audit soient séparées des fonctions opérationnelles. Dans les environnements où un même individu assume des fonctions multiples (par exemple, opérations de sécurité et d'administration), les tâches peuvent être assignées de telle sorte qu'un seul individu ne soit pas en mesure d'exercer un contrôle de bout en bout sur un processus sans un point de contrôle indépendant. Par exemple, la responsabilité de la configuration et la responsabilité de l'approbation des changements doivent être assignées à des individus séparés.

Remarque : *Pour certaines entités, ces meilleures pratiques sont également des conditions pour veiller à la conformité continue de la norme PCI DSS. Par exemple, la norme PCI DSS comprend ces principes dans certaines conditions et la validation complémentaire des entités désignées (Annexe A3 de la norme PCI DSS) exige que les entités désignées valident ces principes.*

Toutes les organisations doivent envisager l'implémentation de ces meilleures pratiques dans leur environnement, même lorsqu'elles ne sont pas tenues de les valider.

Pour les évaluateurs : Échantillonnage des installations de l'entreprise et des composants de système

L'échantillonnage est une option qui permet de faciliter le processus d'évaluation pour les évaluateurs lorsqu'il existe un grand nombre d'installations commerciales et/ou de composants de système.

Bien qu'il soit acceptable qu'un évaluateur échantillonne les composants de système/installation commerciale dans le cadre de son analyse de la conformité d'une entité à la norme PCI DSS, il n'est pas acceptable qu'une entité applique les conditions de la norme PCI DSS uniquement à un échantillon de son environnement (par exemple, les conditions d'analyse de vulnérabilité trimestrielle s'appliquent à tous les composants de système). De même, il n'est pas acceptable qu'un évaluateur examine uniquement un échantillon des conditions de la norme PCI DSS pour déterminer la conformité.

Après avoir considéré le champ d'application global et la complexité de l'environnement évalué, l'évaluateur peut sélectionner de manière indépendante des échantillons des installations de l'entreprise et des composants de système afin d'évaluer la conformité aux conditions PCI DSS. Ces échantillons doivent d'abord être définis pour les installations de l'entreprise puis pour les composants de système, au sein de chaque installation sélectionnée. Les échantillons doivent être représentatifs de tous les types et de tous les emplacements des installations de l'entreprise et des types de composants de système, au sein des installations sélectionnées. Les échantillons doivent être suffisamment importants pour donner à l'évaluateur la garantie que les contrôles sont appliqués comme prévu.

Les exemples d'installations d'entreprise comprennent, sans s'y limiter : les bureaux d'entreprise, les sites en franchise, les installations de traitement, les centres de données et autres types d'installations à des sites différents. L'échantillonnage doit inclure les composants de système au sein de chaque installation de l'entreprise. Par exemple, pour chaque installation de l'entreprise sélectionnée, il convient d'inclure divers systèmes d'exploitation, fonctions et applications liés au domaine évalué.

Au sein de chaque installation de l'entreprise, l'évaluateur peut choisir les serveurs Sun exécutant le navigateur Apache, les serveurs Windows exécutant Oracle, les systèmes d'unités centrales exécutant les applications traditionnelles de traitement de cartes, les serveurs de transfert de données exécutant HP-UX et les serveurs Linux exécutant MySQL. Si toutes les applications s'exécutent à partir d'un système d'exploitation unique (par exemple, Windows 7 ou Solaris 10), l'échantillon doit tout de même inclure diverses applications (par exemple serveurs de bases de données, serveurs Web et serveurs de transfert de données).

Lorsqu'ils choisissent des échantillons d'installations d'entreprise et de composants de système de manière indépendante, les évaluateurs doivent prendre en compte les facteurs suivants :

- S'il existe des processus de contrôles opérationnels et de sécurité PCI DSS standardisés et centralisés sont mis en place pour garantir la cohérence et que chaque installation de l'entreprise/composant du système doit suivre, l'échantillon peut être plus petit que si aucun processus/contrôle n'est en place. L'échantillon doit être assez important pour donner à l'évaluateur une garantie raisonnable que toutes les installations de l'entreprise et tous composants de système sont configurés conformément aux processus standards. L'évaluateur doit vérifier que les contrôles standardisés et centralisés sont mis en œuvre et fonctionnent correctement

- S'il existe plus d'un type de processus de sécurité et/ou opérationnel en place (par exemple pour divers types d'installations de l'entreprise/composants de système), l'échantillon doit être assez important pour intégrer les installations de l'entreprise/composants de système sécurisés par chaque type de processus.
- S'il n'existe pas de processus et contrôles PCI DSS standards en place et que chaque installation de l'entreprise et chaque composant du système sont gérés par des processus non standards, l'échantillon doit être plus important pour que l'évaluateur ait la garantie que chaque installation de l'entreprise/composant du système a mis en œuvre les conditions de la norme PCI DSS de la manière appropriée.
- Les échantillons de composants de système doivent comprendre chaque type et chaque combinaison en utilisation. Par exemple, quand les applications sont échantillonnées, l'échantillon doit comprendre toutes les versions et plateformes pour chaque type d'application.

Lorsque l'échantillonnage est utilisé, l'évaluateur doit, pour chaque échantillon :

- documenter la justification de la technique d'échantillonnage et de la taille de l'échantillon ;
- documenter et valider les processus et contrôles PCI DSS standardisés, utilisés pour déterminer la taille de l'échantillon ;
- expliquer dans quelle mesure l'échantillon est approprié et représentatif de la population globale.

Se référer également à :
Annexe D : Segmentation et échantillonnage des installations de l'entreprise et des composants de système

Les évaluateurs doivent revalider la justification de l'échantillonnage pour chaque évaluation. Si l'échantillonnage est utilisé, divers échantillons des installations de l'entreprise et des composants de système doivent être sélectionnés pour chaque évaluation.

Contrôles compensatoires

Une fois par an, tous les contrôles compensatoires doivent être documentés, examinés et validés par l'évaluateur, puis inclus dans le Rapport sur la conformité qui est envoyé, conformément à *l'annexe B : Contrôles compensatoires* et *annexe C : Fiche de contrôles compensatoires*.

Pour chaque contrôle compensatoire, la fiche de contrôles compensatoires (*annexe C*) **doit** être complétée. Par ailleurs, les résultats des contrôles compensatoires doivent être documentés dans le Rapport sur la conformité, dans la section de la condition PCI DSS correspondante.

Pour plus d'informations sur les « contrôles compensatoires », consulter les *annexes B* et *C* mentionnées ci-dessus.

Instructions et contenu du Rapport sur la conformité

Les instructions et le contenu du Rapport sur la conformité (Report on Compliance, ROC) sont fournis dans le *Modèle de rapport ROC PCI DSS*.

Le *Modèle de rapport ROC PA-DSS* doit être utilisé comme modèle pour créer le *Rapport de conformité*. L'entité évaluée doit respecter les conditions respectives de chaque marque de carte de paiement en matière de rapports pour s'assurer que chaque marque connaît l'état de conformité de l'entité. Contacter chaque marque de paiement ou l'acquéreur pour déterminer les instructions et ses conditions en matière de rapports.

Processus d'évaluation de la norme PCI DSS

Le processus d'évaluation de la norme PCI DSS suppose l'exécution des étapes suivantes :

1. Confirmer le champ d'application de l'évaluation de la norme PCI DSS.
2. Effectuer l'évaluation de l'environnement selon la norme PCI DSS en suivant les procédures de test de chaque condition.
3. Remplir le rapport applicable pour l'évaluation (à savoir Questionnaire d'auto-évaluation (Self-Assessment Questionnaire, SAQ) ou Rapport sur la conformité (ROC)), y compris la documentation concernant tous les contrôles compensatoires, selon les directives et les instructions PCI applicables.
4. Compléter l'intégralité de l'attestation de conformité, pour les prestataires de services ou les commerçants, selon le cas. Les attestations de conformité sont disponibles sur le site Web du PCI SSC.
5. Envoyer le SAQ ou ROC et l'Attestation de conformité, ainsi que toute autre documentation requise, comme les rapports d'analyse ASV, à l'acquéreur (dans le cas de commerçants), à la marque de carte de paiement ou à tout autre demandeur (dans le cas de prestataires de services).
6. Si besoin, effectuer les actions de réparation pour traiter les conditions qui ne sont pas en place, et fournissez un rapport mis à jour.

Versions de PCI DSS

La norme PCI DSS v3.1 est valide à compter de la date de publication de ce document jusqu'au 31 octobre 2016. Après cette date, elle sera retirée. Après cette date, toutes les validations de la norme PCI DSS doivent correspondre à PCI DSS v3.2 ou ultérieure.

La tableau suivant récapitule les versions de la norme PCI DSS et leurs dates d'entrée en vigueur⁶.

Version	Publication :	Retrait :
PCI DSS v3.2 (ce document)	Avril 2016	À déterminer
PCI DSS v3.1	Avril 2015	31 octobre 2016

⁶ Il est susceptible d'être modifié lorsqu'une nouvelle version de PCI DSS est publiée.

Conditions et procédures d'évaluation de sécurité détaillées de la norme PCI DSS

Les informations suivantes définissent les en-têtes de colonnes pour les Conditions et procédures d'évaluation de sécurité de la norme PCI DSS :

- **Conditions de la norme PCI DSS** – Cette colonne définit les conditions de la Norme de sécurité des données, la conformité sera validée au regard de ces conditions.
- **Procédures de test** – Cette colonne indique les processus que l'évaluateur doit suivre pour valider que les conditions de la norme PCI DSS ont été respectées et sont « en place ».
- **Directive** – Cette colonne décrit le but ou l'objectif de sécurité derrière chaque condition de la norme PCI DSS. Cette colonne contient uniquement des directives et elle est destinée à aider à comprendre le but de chaque condition. La directive indiquée dans cette colonne ne remplace et n'étend pas les conditions de la norme PCI DSS ou les procédures de test.

Remarque : Les conditions de la norme PCI DSS ne doivent pas être considérées comme étant en place si les contrôles n'ont pas encore été mis en œuvre ou doivent être terminés à une date future. Une fois que tous les éléments ouverts ou les éléments n'étant pas mis en place ont été adressés par l'entité, l'évaluateur doit procéder de nouveau à l'évaluation afin de valider que la résolution est complétée et vérifier que toutes les conditions sont satisfaites.

Veillez consulter les ressources suivantes (disponibles sur le site Web du PCI SSC) pour documenter l'évaluation PCI DSS :

- Pour découvrir les instructions sur la compilation de rapports de conformité (ROC), consulter le Modèle de rapport ROC PCI DSS.
- Pour découvrir les instructions pour remplir les questionnaires d'auto-évaluation (SAQ), consulter les Directives et instructions SAQ PCI DSS.
- Pour découvrir les instructions sur la soumission des rapports de validation de conformité PCI DSS, consulter Attestations de conformité PCI DSS.

Création et gestion d'un réseau et d'un système sécurisés

Condition 1 : Installer et gérer une configuration de pare-feu pour protéger les données de titulaires de carte

Les pare-feu sont des dispositifs qui contrôlent le trafic autorisé entre le réseau d'une entreprise (interne) et les réseaux non approuvés (externes), ainsi que le trafic entrant et sortant dans des zones plus sensibles du réseau approuvé interne d'une société. L'environnement des données de titulaires de carte est un exemple de zone plus sensible au sein du réseau approuvé d'une entreprise.

Un pare-feu examine l'ensemble du trafic réseau et bloque les transmissions qui ne satisfont pas aux critères de sécurité définis.

Tous les systèmes doivent être protégés contre les accès non autorisés depuis un réseau non approuvé, que ce soit en entrée via Internet (par exemple commerce électronique, accès des employés à Internet à partir de leurs navigateurs, accès des employés à la messagerie électronique, connexions dédiées telles que les connexions inter-entreprises) ou bien via les réseaux sans-fil ou d'autres sources. Les chemins d'accès de/vers des réseaux non approuvés, en apparence insignifiants, peuvent souvent constituer des chemins d'accès non protégés à des systèmes critiques. Les pare-feu sont des mécanismes de protection essentiels sur tout réseau informatique.

D'autres composants de système peuvent assurer une fonctionnalité pare-feu, à condition que ces composants remplissent les conditions minimales des pare-feu définies par la condition 1. Lorsque d'autres composants de système sont utilisés dans l'environnement des données de titulaires de carte pour assurer une fonctionnalité pare-feu, ces dispositifs doivent être inclus dans le champ d'application de l'évaluation de la condition 1.

Conditions PCI DSS	Procédures de test	Directive
1.1 Établissement et mise en œuvre des normes de configuration des pare-feu et des routeurs comprenant les éléments suivants :	1.1 Inspecter les normes de configuration de pare-feu et de routeurs et autres documents spécifiés ci-dessous pour vérifier que les normes sont complètes et mises en œuvre comme suit :	Les pare-feu et les routeurs sont les composants essentiels de l'architecture contrôlant les entrées et les sorties d'un réseau. Il s'agit de dispositifs logiciels ou matériels qui bloquent les accès indésirables et gèrent l'accès autorisé vers et hors du réseau. Les normes et procédures de configuration aideront à garantir que la première ligne de défense de l'organisation en matière de protection des données demeure robuste.
1.1.1 Processus formel d'approbation et de test de toutes les connexions réseau et des modifications apportées aux configurations des pare-feu et des routeurs	1.1.1.a Examiner les procédures documentées pour vérifier qu'un processus formel de test et d'approbation est présent pour : <ul style="list-style-type: none"> • Toutes les connexions du réseau et • Toutes les modifications de pare-feu et de routeur. 	Un processus mis en œuvre et documenté pour l'approbation et le test de toutes les connexions et des modifications apportées aux configurations des pare-feu et des routeurs permettront d'éviter les problèmes de sécurité dus aux erreurs de configuration du réseau, du routeur ou du pare-feu. Sans procédure formelle d'approbation et de test
	1.1.1.b Pour obtenir un échantillon des connexions du réseau, interroger le personnel responsable et examiner les archives	

Conditions PCI DSS	Procédures de test	Directive
	afin de vérifier que les connexions de réseau ont été approuvées et testées.	des modifications, les archives des modifications sont susceptibles de ne pas être mises à jour, ce qui risque de provoquer des incohérences entre la documentation du réseau et la configuration effective.
	1.1.1.c Identifier un échantillon d'une modification effectivement apportée aux configurations de pare-feu et de routeur, comparer à la modification des archives et interroger le personnel responsable pour vérifier que les changements ont été approuvés et testés	
1.1.2 Diagramme du réseau actuel qui identifie toutes les connexions entre l'environnement de données de titulaires de carte et les autres réseaux, y compris tout réseau sans-fil	1.1.2.a Examiner le ou les diagrammes et observer les configurations de réseau pour vérifier qu'un diagramme du réseau actuel existe bien et qu'il documente toutes les connexions aux données de titulaires de carte, y compris tout réseau sans-fil.	Les diagrammes de réseau décrivent comment les réseaux sont configurés et identifient les emplacements des tous les périphériques du réseau. Sans les diagrammes du réseau actuel, des dispositifs pourraient être négligés et inconsciemment laissés en dehors des contrôles de sécurité implémentés pour la norme PCI DSS et, par conséquent, être vulnérables aux attaques.
	1.1.2.b Interroger le personnel responsable pour vérifier que le diagramme est tenu à jour.	
1.1.3 Diagramme actuel montrant le flux des données de titulaires de carte dans les systèmes et les réseaux	1.1.3 Examiner le diagramme des flux de données et interroger le personnel pour vérifier que le diagramme : <ul style="list-style-type: none"> • Montre le flux des données de titulaires de carte dans les systèmes et les réseaux. • Est conservé à jour et mis à jour si besoin suite aux changements de l'environnement. 	Les diagrammes de flux de données de titulaires de carte identifient l'emplacement de toutes les données de titulaires de carte qui sont enregistrées, traitées ou transmises dans le réseau. Les diagrammes de réseau et de flux de données aident une organisation à comprendre et à suivre la portée de leur environnement, en montrant comment les données de titulaires de carte circulent dans les réseaux et entre les systèmes et les dispositifs individuels.
1.1.4 Conditions relatives au pare-feu au niveau de chaque connexion Internet et entre toute zone démilitarisée (DMZ) et la zone de réseau interne	1.1.4.a Examiner les Normes de configuration de pare-feu et vérifier qu'elles comprennent les conditions relatives au pare-feu au niveau de chaque connexion Internet et entre toute DMZ et la zone de réseau interne.	L'utilisation d'un pare-feu sur chaque connexion Internet entrante (et sortante) du réseau et entre toute DMZ et le réseau interne permet à l'organisation de surveiller et de contrôler les accès et de réduire les risques qu'un individu malveillant parvienne à accéder au réseau interne
	1.1.4.b Vérifier que le diagramme de réseau actuel est conforme aux normes de configuration des pare-feu.	

Conditions PCI DSS	Procédures de test	Directive
	<p>1.1.4.c Observer les configurations de réseau pour vérifier qu'un pare-feu est en place à chaque connexion Internet et entre toute zone démilitarisée (demilitarized zone, DMZ) et la zone de réseau interne, conformément aux normes de configuration documentées et aux diagrammes de réseau.</p>	<p>grâce à une connexion non protégée.</p>
<p>1.1.5 Description des groupes, des rôles et des responsabilités pour la gestion des composants du réseau</p>	<p>1.1.5.a Vérifier que les normes de configuration des pare-feu et des routeurs comprennent une description des groupes, des rôles et des responsabilités pour la gestion des composants réseau.</p>	<p>Cette description des rôles et affectation des responsabilités garantit que le personnel sait qui est responsable de la sécurité de tous les composants du réseau et que ceux à qui la gestion des composants est affectée connaissent leurs responsabilités. Si les rôles et les responsabilités ne sont pas assignés de manière formelle, des dispositifs pourraient demeurer sans gestion.</p>
	<p>1.1.5.b Interroger le personnel auquel responsable de la gestion des composants du réseau pour confirmer que les rôles et les responsabilités sont affectés ainsi qu'il est documenté.</p>	
<p>1.1.6 Documentation de la justification professionnelle et approbation de l'utilisation de tous les services, protocoles et ports autorisés, y compris la documentation des fonctions de sécurité mises en œuvre pour les protocoles considérés comme étant non sécurisés.</p>	<p>1.1.6.a Vérifier que les normes de configuration du pare-feu et du routeur comprennent une liste documentée des services, des protocoles et des ports, y compris la justification commerciale et l'approbation pour chacun de ces éléments.</p>	<p>Les risques sont souvent dus à la présence de services et de ports non utilisés dans la mesure où ces derniers ont souvent des vulnérabilités connues et beaucoup d'organisations ne corrigent pas les vulnérabilités des services, protocoles et ports qu'elles n'utilisent pas (même si les vulnérabilités existent bien). En définissant et en documentant clairement les services, les protocoles et les ports nécessaires à la conduite de leurs activités, les organisations peuvent s'assurer que tous les autres services, protocoles et ports sont désactivés ou éliminés.</p> <p>Un personnel indépendant du personnel chargé de gérer la configuration doit attribuer les approbations.</p> <p>Si des services, protocoles ou ports non sécurisés sont nécessaires à l'entreprise, le risque inhérent à l'utilisation de ces protocoles doit être clairement compris et accepté par l'organisation. L'utilisation du protocole doit être justifiée et les fonctions de sécurité permettant l'utilisation sécurisée de ces protocoles doivent être documentées et appliquées. Si ces services, protocoles ou ports non sécurisés ne sont pas</p>
	<p>1.1.6.b Identifier les services, protocoles et ports non sécurisés autorisés, et vérifier que les fonctions de sécurité sont documentées pour chaque service.</p>	
	<p>1.1.6.c Examiner les configurations de pare-feu et de routeur pour vérifier que les fonctions de sécurité documentées sont mises en œuvre pour chaque service, protocole ou port non sécurisé.</p>	

Conditions PCI DSS	Procédures de test	Directive
		<p>nécessaires à l'entreprise, ils doivent être désactivés ou supprimés.</p> <p>Pour obtenir des directives sur les services, protocoles ou ports jugés comme non sécurisés, se reporter aux normes et directives (par exemple, NIST, ENISA, OWASP, etc.).</p>
<p>1.1.7 Exigence d'analyse des règles concernant les pare-feu et les routeurs au moins tous les six mois</p>	<p>1.1.7.a Vérifier que les normes de configuration des pare-feu et des routeurs exigent l'examen des règles des pare-feu et des routeurs au moins tous les six mois.</p> <p>1.1.7.b Examiner la documentation relative aux examens des règles interroger le personnel responsable pour vérifier que les règles sont passées en revue au moins tous les six mois.</p>	<p>Cet examen donne à l'organisation une occasion, au moins tous les six mois, d'éliminer les règles superflues, obsolètes ou incorrectes et de s'assurer que toutes les règles n'admettent que les services et les ports autorisés correspondants aux besoins documentés de l'activité.</p> <p>Les organisations qui connaissent un volume important de changement de règles de pare-feu et de routeur peuvent souhaiter effectuer des analyses plus fréquemment, pour s'assurer que les règles continuent de répondre aux besoins de l'entreprise.</p>
<p>1.2 Créer des configurations de pare-feu et de routeur qui limitent les connexions entre les réseaux non approuvés et tous les composants de système dans l'environnement des données de titulaires de carte.</p> <p>Remarque : Un « réseau non approuvé » est tout réseau externe aux réseaux appartenant à l'entité sous investigation et/ou qui n'est pas sous le contrôle ou la gestion de l'entité.</p>	<p>1.2 Examiner les configurations des pare-feu et des routeurs et suivre la procédure suivante pour vérifier que les connexions sont restreintes entre les réseaux non approuvés et les composants de système dans l'environnement des données de titulaires de carte :</p>	<p>Il est essentiel d'installer une protection réseau entre le réseau approuvé interne et tout autre réseau non approuvé externe et/ou échappant au contrôle ou à la gestion de l'entreprise. Si cette mesure n'est pas correctement mise en place, l'entité sera exposée au risque d'intrusion d'individus ou de logiciels malveillants.</p> <p>Pour que la fonction de pare-feu soit efficace, elle doit être configurée correctement pour contrôler et/ou limiter le trafic entrant et sortant du réseau de l'entité.</p>
<p>1.2.1 Restreindre le trafic entrant et sortant au trafic nécessaire à l'environnement des données de titulaires de carte et, particulièrement, refuser tout autre trafic.</p>	<p>1.2.1.a Examiner les normes de configuration de routeur et de pare-feu pour vérifier qu'ils identifient le trafic entrant et sortant nécessaire pour l'environnement de données de titulaires de carte.</p> <p>1.2.1.b Examiner les configurations de routeur et de pare-feu pour vérifier que le trafic entrant et sortant est limité au trafic nécessaire à l'environnement des données de titulaires de</p>	<p>L'examen de toutes les connexions entrantes ou sortantes permet d'inspecter et de restreindre le trafic selon l'adresse source et/ou de destination, ce qui permet d'empêcher l'accès non filtré entre les environnements non approuvés et approuvés. Cela empêche les individus malveillants de pénétrer le réseau de l'entité par le biais</p>

Conditions PCI DSS	Procédures de test	Directive
	<p>carte.</p> <p>1.2.1.c Examiner les configurations de pare-feu et de routeur pour vérifier que tous les autres trafics entrants et sortants sont explicitement refusés, par exemple à l'aide d'une instruction « refuser tout » explicite ou d'un refus implicite après une instruction d'autorisation.</p>	<p>d'adresses IP non autorisées, ou d'utiliser des services, protocoles ou ports de manière non autorisée (par exemple, pour transmettre des données obtenues sur le réseau de l'entité vers un serveur non approuvé).</p> <p>Mettre en œuvre une règle qui refuse tout trafic entrant ou sortant qui n'est pas nécessaire aide à empêcher les brèches par négligence qui pourraient permettre un trafic entrant ou sortant indésirable et potentiellement dommageable.</p>
<p>1.2.2 Sécuriser et synchroniser les fichiers de configuration des routeurs.</p>	<p>1.2.2.a Examiner les fichiers de configuration du routeur pour vérifier qu'ils sont sécurisés contre un accès non autorisé.</p> <p>1.2.2.b Examiner les configurations de routeur pour vérifier qu'elles sont synchronisées, par exemple, la configuration de fonctionnement (ou active) correspond à la configuration de démarrage (utilisée lorsque les machines sont mises en route).</p>	<p>Lorsque les fichiers de configuration de routeur en cours de fonctionnement (ou actifs) comprennent les réglages actuels actifs, les fichiers de démarrage (qui sont utilisés lorsque les routeurs sont redémarrés ou démarrés) doivent être mis à jour avec les mêmes réglages sécurisés pour assurer que ces réglages sont appliqués lorsque la configuration de démarrage est exécutée.</p> <p>Puisqu'ils ne fonctionnent que de temps en temps, les fichiers de configuration de démarrage sont souvent oubliés et ne sont pas mis à jour. Lorsqu'un routeur redémarre et charge une configuration de démarrage qui n'a pas été mise à jour avec les mêmes réglages sécurisés que ceux de la configuration en fonctionnement, les règles pourraient être moins strictes et permettre l'accès d'un individu malveillant au réseau.</p>
<p>1.2.3 Installer des pare-feu de périmètre entre tous les réseaux sans-fil et l'environnement des données de titulaires de carte, et configurer ces pare-feu pour refuser ou, s'il est nécessaire à des fins professionnelles, autoriser uniquement le trafic entre l'environnement sans-fil et l'environnement de données de titulaires de carte.</p>	<p>1.2.3.a Examiner les configurations de pare-feu et de routeur pour vérifier que des pare-feu de périmètre sont installés entre tous les réseaux sans-fil et l'environnement des données de titulaires de carte.</p> <p>1.2.3.b Vérifier que les pare-feu refusent ou, si ce trafic est nécessaire à des fins commerciales, permettent uniquement au trafic autorisé de circuler entre l'environnement du réseau sans-fil et l'environnement des données de titulaires de carte.</p>	<p>La mise en œuvre et l'exploitation connues (ou inconnues) de la technologie sans-fil sur un réseau sont souvent la voie qu'utilisent les individus malveillants pour accéder au réseau et aux données de titulaires de carte. Si un périphérique ou un réseau sans-fil est installé à l'insu d'une entreprise, un individu malveillant peut pénétrer dans le réseau de manière « invisible ». Si les pare-feu ne restreignent pas l'accès des réseaux sans-fil dans le CDE, les individus malveillants qui accèdent au réseau sans-fil sans</p>

Conditions PCI DSS	Procédures de test	Directive
		<p>autorisation peuvent facilement se connecter au CDE et compromettre les informations de comptes.</p> <p>Des pare-feu doivent être installés entre tous les réseaux sans-fil et l'environnement des données de titulaires de carte, indépendamment de l'objectif de l'environnement auquel le réseau sans-fil est connecté. Ceci peut inclure notamment les réseaux d'entreprise, les magasins de détail, les réseaux d'hôte, les environnements d'entrepôt, etc.</p>
<p>1.3 Interdire l'accès public direct entre Internet et tout composant du système dans l'environnement des données de titulaires de carte.</p>	<p>1.3 Examiner les configurations des pare-feu et des routeurs – y compris notamment, le routeur interne au niveau d'Internet, le routeur et le pare-feu DMZ, le segment DMZ du titulaire, le routeur du périmètre et le segment du réseau interne du titulaire et suivez la procédure décrite ci-après afin de déterminer qu'il n'existe aucun accès direct entre Internet et les composants de système dans le segment du réseau interne du titulaire :</p>	<p>Bien que certaines raisons légitimes puissent exister pour expliquer l'autorisation de certaines connexions non autorisées aux systèmes DMZ (par exemple, l'autorisation d'un accès public à un serveur Web), de telles connexions ne doivent jamais être attribuées aux systèmes sur le réseau interne. L'objectif d'un pare-feu consiste à gérer et contrôler toutes les connexions entre les systèmes publics et les systèmes internes, en particulier ceux qui stockent, traitent ou transmettent des données de titulaires de carte. Si un accès direct est autorisé entre les systèmes publics et le CDE, les protections assurées par le pare-feu sont contournées et les composants de système stockant les données de titulaires de carte peuvent être compromis.</p>
<p>1.3.1 Déployer une DMZ pour limiter le trafic entrant aux seuls composants de système fournissant des services, protocoles et ports autorisés, accessibles au public.</p>	<p>1.3.1 Examiner les configurations de pare-feu et de routeur pour vérifier qu'une DMZ est déployée pour limiter le trafic entrant aux seuls composants de système fournissant des services, protocoles et ports autorisés, accessibles au public.</p>	<p>La DMZ est la partie du réseau qui gère les connexions entre Internet (ou tout autre réseau non approuvé) et les services internes qu'une entreprise doit mettre à la disposition du public (comme un serveur Web).</p>
<p>1.3.2 Limiter le trafic Internet entrant aux adresses IP dans la DMZ.</p>	<p>1.3.2 Examiner les configurations de pare-feu et de routeur pour vérifier que le trafic Internet entrant est limité aux adresses IP dans la DMZ.</p>	<p>Cette fonction est destinée à empêcher des individus malveillants d'accéder au réseau interne de l'entreprise à partir d'Internet ou d'utiliser des services, des protocoles ou des ports de manière non autorisée.</p>

Conditions PCI DSS	Procédures de test	Directive
<p>1.3.3 Mise en œuvre des mesures anti-usurpation pour détecter et pour empêcher les adresses IP de source frauduleuse de pénétrer sur le réseau.</p> <p>(Par exemple, bloquer le trafic originaire d'Internet avec une adresse de source interne).</p>	<p>1.3.3 Examiner les configurations de pare-feu et de routeur pour vérifier que les mesures anti-usurpation sont mises en œuvre, par exemple, les adresses internes ne peuvent pas passer d'Internet vers la DMZ.</p>	<p>Normalement, un paquet contient l'adresse IP de l'ordinateur qui l'a envoyé aux autres ordinateurs à l'origine, de manière à ce que les autres ordinateurs du réseau sachent d'où vient le paquet. Les individus malveillants essayeront souvent d'usurper (ou d'imiter) l'adresse IP d'expédition pour que le système cible pense que le paquet provient d'une source autorisée.</p> <p>Le filtrage des paquets entrant dans le réseau aide, entre autres, à garantir que les paquets ne sont pas « usurpés » pour ressembler aux paquets provenant du réseau interne de l'organisation.</p>
<p>1.3.4 Ne pas autoriser le trafic sortant non autorisé de l'environnement des données de titulaires de carte vers Internet.</p>	<p>1.3.4 Examiner les configurations de pare-feu et de routeur pour vérifier que le trafic sortant de l'environnement des données de titulaires de carte vers Internet est expressément autorisé.</p>	<p>Tout le trafic sortant, issu de l'environnement des données de titulaires de carte, doit être évalué afin de s'assurer qu'il suit toutes les règles établies et autorisées. Les connexions doivent subir une inspection afin de restreindre le trafic aux seules communications autorisées (par exemple en limitant les adresses/ports sources ou de destination et/ou en bloquant le contenu).</p>
<p>1.3.5 Les connexions « établies » sont les seules autorisées sur le réseau.</p>	<p>1.3.5 Examiner les configurations de pare-feu et de routeur pour vérifier que le pare-feu autorise uniquement les connexions établies sur le réseau interne et refuse toute connexion entrante non associée à une session établie précédemment.</p>	<p>Un pare-feu, qui maintient « l'état » (ou le statut) pour chaque connexion via le pare-feu, sait si une réponse apparente à une connexion précédente est réellement une réponse valide et autorisée (puisque'il conserve le statut de chaque connexion) ou s'il s'agit d'un trafic malveillant qui essaye de tromper le pare-feu pour qu'il accepte la connexion.</p>

Conditions PCI DSS	Procédures de test	Directive
<p>1.3.6 Placer les composants de système qui stockent les données de titulaires de carte (comme une base de données) dans une zone de réseau interne, isolée de la DMZ et des autres réseaux non approuvés.</p>	<p>1.3.6 Examiner les configurations de pare-feu et de routeur pour vérifier que les composants de système qui stockent les données de titulaires de carte se trouvent dans une zone de réseau interne, isolée de la DMZ et des autres réseaux non approuvés.</p>	<p>Si les données de titulaires de carte se trouvent dans la DMZ, il est plus facile pour les pirates externes d'accéder à ces informations, puisqu'il a moins de couches à pénétrer. Sécuriser les composants de système qui stockent les données de titulaires de carte dans une zone de réseau externe qui est séparée de la DMZ et des autres réseaux non autorisés par un pare-feu peut empêcher le trafic non autorisé du réseau d'atteindre le composant du système.</p> <p>Remarque : Cette condition n'est pas destinée à être appliquée au stockage temporaire des données de titulaires de carte dans la mémoire volatile.</p>
<p>1.3.7 Ne pas divulguer les adresses IP et les informations d'acheminement confidentielles à des parties non autorisées.</p> <p>Remarque : Quelques-unes des méthodes permettant de dissimuler les adresses IP sont présentées ci-après :</p> <ul style="list-style-type: none"> • Traduction d'adresse réseau (Network Address Translation, NAT) ; • Protéger les serveurs contenant des données de titulaires de carte derrière des serveurs proxy/pare-feu ; • Retrait ou filtrage des annonces d'acheminement pour les réseaux privés employant des adresses enregistrées ; • Utilisation interne de l'espace d'adresse RFC1918 au lieu d'adresses enregistrées. 	<p>1.3.7.a Examiner les configurations de pare-feu et de routeur pour vérifier que des moyens sont en place pour prévenir la divulgation d'adresses IP et d'informations d'acheminement confidentielles depuis des réseaux internes sur Internet.</p> <p>1.3.7.b Interroger le personnel et examiner la documentation pour vérifier que toute divulgation d'adresses IP et d'informations d'acheminement confidentielles à des entités externes est autorisée.</p>	<p>Restreindre la diffusion des adresses IP internes ou privées est essentiel pour empêcher un pirate « d'apprendre » les adresses IP du réseau interne et d'utiliser cette information pour accéder au réseau.</p> <p>Les méthodes utilisées pour remplir cette condition varient en fonction de la technologie réseau spécifique utilisée. Par exemple, les contrôles utilisés pour satisfaire à cette condition peuvent différer entre des réseaux IPv4 et IPv6.</p>

Conditions PCI DSS	Procédures de test	Directive
<p>1.4 Installer un logiciel de pare-feu personnel ou une fonctionnalité équivalente sur tout appareil informatique portable (y compris les appareils appartenant à la société et/ou à l'employé) qui se connecte à Internet en dehors du réseau (par exemple, les ordinateurs portables utilisés par les employés) et qui permet également un accès au CDE. Les configurations de pare-feu (ou fonctionnalité équivalente) comprennent ce qui suit :</p> <ul style="list-style-type: none"> • Des réglages de configuration spécifiques sont définis. • Un pare-feu personnel (ou fonctionnalité équivalente) fonctionne activement. • Le pare-feu personnel (ou fonctionnalité équivalente) ne peut pas être altéré par les utilisateurs des appareils informatiques portables. 	<p>1.4.a Examiner les politiques et les normes de configuration pour vérifier :</p> <ul style="list-style-type: none"> • Un logiciel de pare-feu personnel ou une fonctionnalité équivalente est requis(e) pour tous les appareils informatiques portables (y compris les appareils appartenant à la société et/ou à l'employé) qui se connectent à Internet en dehors du réseau (par exemple, les ordinateurs portables utilisés par les employés) et qui permettent également un accès au CDE. • Les réglages de configuration spécifiques sont définis pour le pare-feu personnel (ou fonctionnalité équivalente). • Le pare-feu personnel (ou fonctionnalité équivalente) est configuré pour un fonctionnement actif. • Le pare-feu personnel (ou fonctionnalité équivalente) est configuré de manière à ne pas être altéré par les utilisateurs des appareils informatiques portables. <p>1.4.b Inspecter un échantillon des appareils détenus par la société et/ou les employés pour vérifier que :</p> <ul style="list-style-type: none"> • Un logiciel de pare-feu personnel (ou fonctionnalité équivalente) est installé et configuré selon les réglages de configuration spécifiques de l'organisation. • Un pare-feu personnel (ou fonctionnalité équivalente) fonctionne activement. • Le pare-feu personnel (ou fonctionnalité équivalente) ne peut pas être altéré par les utilisateurs des appareils informatiques portables. 	<p>Les appareils informatiques portables qui peuvent se connecter à Internet depuis l'extérieur du pare-feu de l'entreprise sont plus vulnérables aux menaces basées sur Internet. Le recours à la fonctionnalité de pare-feu (par exemple, le logiciel ou le matériel de pare-feu personnel) permet de protéger les appareils des attaques originaires d'Internet, qui pourraient utiliser l'appareil pour accéder aux systèmes et aux données de l'organisation une fois que l'appareil est à nouveau connecté au réseau.</p> <p>Les réglages spécifiques de configuration de pare-feu sont déterminés par l'organisation.</p> <p>Remarque : Cette condition s'applique aux appareils informatiques portables détenus par les employés et la société. Les systèmes, dont la gestion n'est pas conforme à la politique de l'entreprise, sont sources de faiblesses et procurent aux individus malveillants des opportunités à exploiter. Permettre aux systèmes non autorisés de se connecter au CDE d'une organisation pourrait se solder par l'accès aux pirates et autres utilisateurs malveillants.</p>
<p>1.5 Assurer que les politiques de sécurité et les procédures opérationnelles pour la gestion des pare-feu sont documentées, utilisées et connues de toutes les parties concernées.</p>	<p>1.5 Examiner la documentation et interroger le personnel pour vérifier que les politiques de sécurité et les procédures opérationnelles pour la gestion des pare-feu sont :</p> <ul style="list-style-type: none"> • Documentées • Utilisées et • Connues de toutes les parties concernées. 	<p>Le personnel doit être conscient et suivre les politiques de sécurité et les procédures opérationnelles pour assurer que les pare-feu et les routeurs sont continuellement gérés de sorte que les accès non autorisés au réseau soient empêchés.</p>

Condition 2 : Ne pas utiliser les mots de passe système et autres paramètres de sécurité par défaut définis par le fournisseur

Les individus malveillants (à l'intérieur ou à l'extérieur d'une entreprise), utilisent souvent les mots de passe et autres paramètres par défaut du fournisseur pour s'infiltrer dans les systèmes en vue de les endommager. Ces mots de passe et paramètres sont bien connus des communautés de pirates et sont facilement détectables à partir d'informations publiques.

Conditions PCI DSS	Procédures de test	Directive
<p>2.1 Changer systématiquement les paramètres par défaut définis par le fournisseur ou désactiver les comptes par défaut inutiles avant d'installer un système sur le réseau.</p> <p>Cette pratique s'applique à TOUS les mots de passe par défaut, y compris, mais sans s'y limiter, les mots de passe utilisés par les systèmes d'exploitation, les logiciels qui assurent des services de sécurité, les comptes d'application et de système, les terminaux de point de vente (<i>point-of-sale</i>, POS), les applications de paiement, les chaînes de communauté de protocoles de gestion de réseau simple (Simple Network Management Protocol, SNMP), etc.</p>	<p>2.1.a Choisir un échantillon des composants de système et essayer d'ouvrir une session (avec l'aide de l'administrateur du système) sur les appareils et applications en utilisant les comptes et mots de passe par défaut fournis par le fournisseur, pour vérifier que TOUS les mots de passe par défaut (y compris ceux des systèmes d'exploitation, des logiciels qui assurent des services de sécurité, des comptes d'application et de système, des terminaux de POS et des chaînes de communauté de protocole de gestion simple de réseau [SNMP]) ont été changés. (Se référer aux manuels du fournisseur et aux sources disponibles sur Internet pour rechercher les comptes/mots de passe définis par le fournisseur.)</p> <p>2.1.b Pour l'échantillon de composants de système, vérifier que tous les comptes par défaut inutiles (y compris les comptes utilisés par les systèmes d'exploitation, les applications, les systèmes, les terminaux de POS, SNMP, etc.) sont éliminés ou désactivés.</p> <p>2.1.c Interroger le personnel et examiner la documentation connexe pour vérifier que :</p> <ul style="list-style-type: none"> • Tous les paramètres de fournisseur par défaut (y compris les mots de passe par défaut des systèmes d'exploitation, les logiciels assurant des services de sécurité, les comptes d'application et de système, les terminaux de POS, les chaînes de communauté SNMP, etc.) sont changés avant qu'un système ne soit installé sur le réseau. • Les comptes par défaut inutiles (y compris les comptes utilisés par les systèmes d'exploitation, les applications, les systèmes, les terminaux de POS, SNMP, etc.) sont 	<p>Les individus malveillants (à l'intérieur ou à l'extérieur d'une organisation) utilisent souvent les paramètres par défaut définis par le fournisseur, noms de compte et mots de passe, pour compromettre le logiciel du système d'exploitation, les applications et les systèmes sur lesquels ils sont installés. Dans la mesure où ces paramètres par défaut sont souvent publiés et sont bien connus des communautés de pirates, changer ces paramètres laissera le système moins vulnérable aux attaques.</p> <p>Même si un compte par défaut n'est pas censé être utilisé, changer le mot de passe par défaut pour un mot de passe unique et robuste, puis désactiver le compte, empêchera qu'un individu malveillant puisse réactiver le compte et obtenir un accès avec le mot de passe par défaut.</p>

Conditions PCI DSS	Procédures de test	Directive
<p>2.1.1 Pour les environnements sans-fil connectés à l'environnement des données de titulaires de carte ou qui transmettent des données de titulaires de carte, changer TOUS les paramètres par défaut définis par le fournisseur à l'installation, notamment les clés de cryptage sans-fil, les mots de passe et les chaînes de communauté SNMP.</p>	<p>éliminés ou désactivés avant qu'un système ne soit installé sur le réseau.</p> <p>2.1.1.a Interroger le personnel responsable et examiner la documentation connexe pour vérifier que :</p> <ul style="list-style-type: none"> • Les clés de cryptage ont été modifiées du réglage par défaut lors de l'installation. • Les clés de cryptage par défaut sont modifiées à chaque fois qu'une personne qui les connaît quitte la société ou change de poste. <p>2.1.1.b Interroger le personnel et examiner les politiques et les procédures vérifier que :</p> <ul style="list-style-type: none"> • Les chaînes de communauté SNMP par défaut doivent être modifiées à l'installation. • Les mots de passe/locutions de passage sur des points d'accès doivent être modifiés à l'installation. <p>2.1.1.c Examiner la documentation du fournisseur et ouvrir une session sur les dispositifs sans-fil, avec l'aide de l'administrateur du système, pour vérifier que :</p> <ul style="list-style-type: none"> • Les chaînes de communauté SNMP par défaut ne sont pas utilisées. • les mots/phrases de passe par défaut des points d'accès ne sont pas utilisés. <p>2.1.1.d Examiner la documentation du fournisseur et observer les paramètres de la configuration sans-fil pour vérifier que le firmware des périphériques sans-fil est mis à jour de manière à prendre en charge un cryptage robuste pour :</p> <ul style="list-style-type: none"> • L'authentification des réseaux sans-fil ; • La transmission sur les réseaux sans-fil. <p>2.1.1.e Examiner la documentation du fournisseur et observer les paramètres de configuration sans-fil pour vérifier que les autres paramètres par défaut liés à la sécurité ont été changés, le cas échéant.</p>	<p>Si les réseaux sans-fil ne sont pas déployés avec une configuration de sécurité suffisante (y compris par la modification des paramètres par défaut), des renifleurs sans-fil peuvent intercepter le trafic, capturer facilement des données et des mots de passe et pénétrer sans difficulté le réseau pour l'attaquer.</p> <p>En outre, le protocole d'échange de clés de l'ancienne version de cryptage 802.11x (Wired Equivalent Privacy -confidentialité équivalente aux transmissions par fil WEP) a été décrypté et peut rendre le cryptage inutile. Le firmware des dispositifs doit être mis à jour pour prendre en charge des protocoles plus sécurisés.</p>

Conditions PCI DSS	Procédures de test	Directive
<p>2.2 Élaborer des normes de configuration pour tous les composants de système. S'assurer que ces normes couvrent toutes les vulnérabilités de la sécurité et sont compatibles avec toutes les normes renforçant les systèmes en vigueur dans le secteur.</p> <p>Les sources des normes renforçant les systèmes en vigueur dans le secteur, comprennent, sans s'y limiter, les organismes suivants :</p> <ul style="list-style-type: none"> • Center for Internet Security (CIS – Centre de sécurité Internet) • International Organization for Standardization (ISO – Organisation des normes internationales) • SysAdmin Audit Network Security (SANS) Institute (Institut SANS) • National Institute of Standards Technology (NIST – Institut national des standards et de la technologie) 	<p>2.2.a Examiner les normes de configuration du système de l'organisation pour tous les types de composants de système et vérifier que ces normes sont compatibles avec les normes de renforcement en vigueur dans le secteur.</p> <p>2.2.b Examiner les politiques et interroger le personnel pour vérifier que les normes de configuration du système sont mises à jour au fur et à mesure de l'identification de nouvelles vulnérabilités, qui se trouve dans la condition 6.1.</p> <p>2.2.c Examiner les politiques et interroger le personnel pour vérifier que les normes de configuration du système sont appliquées lorsque de nouveaux systèmes sont configurés et que leur mise en place est vérifiée lorsqu'un système est installé sur le réseau.</p> <p>2.2.d Vérifier que les normes de configuration du système comprennent les procédures suivantes pour tous les types de composants de système :</p> <ul style="list-style-type: none"> • Changer tous les paramètres par défaut fournis par le fournisseur et éliminer tous les comptes par défaut inutiles • Appliquer uniquement une fonction primaire par serveur afin d'éviter la coexistence, sur le même serveur, de fonctions exigeant des niveaux de sécurité différents • Activer uniquement les services, protocoles, démons, etc. nécessaires pour le fonctionnement du système. • Mettre en place des fonctions de sécurité supplémentaires pour tout service, protocole ou démon nécessaires que l'on estime non sécurisés. • Configurer les paramètres de sécurité du système pour empêcher les actes malveillants • Supprimer toutes les fonctionnalités qui ne sont pas nécessaires, par exemple scripts, pilotes, fonctions, sous-systèmes, systèmes de fichiers et serveurs Web superflus. 	<p>De nombreux systèmes d'exploitation, bases de données et applications d'entreprise présentent des points faibles connus et il existe des moyens également connus de les configurer pour résoudre les vulnérabilités de sécurité. Pour aider ceux qui manquent d'expertise en sécurité, un grand nombre d'entreprises de sécurité ont défini des recommandations et des directives visant à renforcer les systèmes, qui expliquent comment corriger ces faiblesses.</p> <p>Les exemples de sources de directives sur les normes de configuration comprennent notamment : www.nist.gov, www.sans.org, et www.cisecurity.org, www.iso.org ainsi que les fournisseurs de produit.</p> <p>Les normes de configuration de système doivent également être conservées à jour afin de garantir que les faiblesses récemment identifiées sont corrigées avant l'installation du système sur le réseau.</p>

Conditions PCI DSS	Procédures de test	Directive
<p>2.2.1 N'appliquer qu'une fonction principale par serveur afin d'éviter la coexistence, sur le même serveur, de fonctions exigeant des niveaux de sécurité différents (Par exemple, les serveurs Web, les serveurs de bases de données et les serveurs DNS doivent être déployés sur des serveurs distincts).</p> <p>Remarque : Lorsque des technologies de virtualisation sont utilisées, n'appliquer qu'une fonction primaire par composant de système virtuel.</p>	<p>2.2.1.a Sélectionner un échantillon de composants de système et inspecter les configurations du système pour vérifier qu'une seule fonction primaire par serveur est implémentée.</p> <p>2.2.1.b Si des technologies de virtualisation sont utilisées, inspecter les configurations de système pour vérifier que seule une fonction primaire est déployée par composant de système ou dispositif virtuel.</p>	<p>Si des fonctions de serveur, qui ont besoin de niveaux de sécurité différents, sont situées sur le même serveur, le niveau de sécurité des fonctions ayant le besoin de sécurité le plus important devra être réduit pas la présence de fonctions à moindre sécurité. En outre, les fonctions de serveur ayant un niveau de sécurité moins important sont susceptibles d'introduire une faiblesse dans les autres fonctions du même serveur. En considérant les besoins de sécurité de différentes fonctions du serveur dans le cadre des normes de configuration du système et des processus connexes, les organisations peuvent assurer que les fonctions qui requièrent des niveaux de sécurité différents ne coexistent pas sur le même serveur.</p>
<p>2.2.2 Activer uniquement les services, protocoles, démons, etc., nécessaires pour le fonctionnement du système.</p>	<p>2.2.2.a Sélectionner un échantillon de composants de système et examiner les démons, les protocoles et les services activés du système pour vérifier que seuls les services ou protocoles nécessaires sont activés.</p> <p>2.2.2.b Identifier tout service, démon, ou protocole actif et non sécurisé et interroger le personnel pour vérifier qu'ils sont justifiés selon les normes de configuration documentées.</p>	<p>Comme indiqué à la condition 1.1.6, une entreprise peut avoir besoin de nombreux protocoles (ou les avoir activés par défaut) et ceux-ci sont fréquemment utilisés par les individus malveillants pour endommager un réseau. Inclure cette condition dans le cadre des normes de configuration d'une organisation et des processus connexes garantit que seuls les services et protocoles nécessaires sont activés.</p>

Conditions PCI DSS	Procédures de test	Directive
<p>2.2.3 Implémenter les fonctions de sécurité supplémentaires pour tout service, protocole ou démon nécessaire et jugé comme non sécurisé.</p> <p>Remarque : Les conditions dans l'annexe A2 doivent être remplies avec l'utilisation du SSL/TLS initial.</p>	<p>2.2.3.a Inspecter les réglages de configuration pour vérifier que les fonctions de sécurité sont documentées et mises en œuvre pour tous les services, démons ou protocoles non sécurisés.</p> <p>2.2.3.b En cas d'utilisation du SSL/TLS initial, suivre les procédures de test dans l'Annexe A2 : <i>Autres conditions de la norme PCI DSS s'appliquant aux entités qui utilisent le SSL/TLS initial.</i></p>	<p>Activer les fonctions de sécurité avant que les nouveaux serveurs ne soient déployés empêchera que des serveurs soient installés dans l'environnement ayant des configurations non sécurisées.</p> <p>Assurer que tous les services, protocoles et démons non sécurisés soient sécurisés à l'aide de fonctions de sécurité appropriées rend la tâche difficile pour les individus malveillants qui cherchent à tirer avantage des points compromis généralement utilisés dans un réseau.</p> <p>Consulter les normes sectorielles et les meilleures pratiques pour obtenir des informations sur une cryptographie robuste et des protocoles sécurisés (par exemple, NIST SP 800-52 et SP 800-57, OWASP, etc.).</p>

Conditions PCI DSS	Procédures de test	Directive
<p>2.2.4 Configurer les paramètres de sécurité du système pour empêcher les actes malveillants.</p>	<p>2.2.4.a Interroger les administrateurs système et/ou les responsables de la sécurité pour vérifier qu'ils connaissent les paramètres de sécurité courants des composants de système.</p> <p>2.2.4.b Examiner les normes de sécurité du système pour vérifier que les paramètres de sécurité courants sont inclus.</p> <p>2.2.4.c Sélectionner un échantillon de composants de système et inspecter les paramètres de sécurité communs pour vérifier qu'ils sont configurés de manière appropriée et selon les normes de configuration.</p>	<p>Les normes de configuration et les processus connexes doivent répondre de manière spécifique aux réglages et aux paramètres qui ont des implications de sécurité connues pour chaque type de système utilisé.</p> <p>Pour que les systèmes soient configurés de manière sécurisée, le personnel responsable de la configuration et/ou de l'administration des systèmes doivent être bien informés des paramètres et des réglages de sécurité spécifiques qui s'appliquent au système.</p>
<p>2.2.5 Supprimer toutes les fonctionnalités qui ne sont pas nécessaires, par exemple scripts, pilotes, fonctions, sous-systèmes, systèmes de fichiers et serveurs Web superflus.</p>	<p>2.2.5.a Sélectionner un échantillon de composants de système et inspecter la configuration pour vérifier que toutes les fonctionnalités qui ne sont pas nécessaires (par exemple scripts, pilotes, fonctions, sous-systèmes, systèmes de fichiers, etc.) sont supprimées.</p> <p>2.2.5.b. Examiner la documentation et les paramètres de sécurité pour vérifier que les fonctions activées sont documentées et prennent en charge une configuration sécurisée.</p> <p>2.2.5.c. Examiner la documentation et les paramètres de sécurité pour vérifier que seules les fonctions documentées sont présentes sur les composants de système échantillonnés.</p>	<p>Les fonctions superflues peuvent apporter une opportunité supplémentaire d'accéder au système pour des individus malveillants. En éliminant les fonctions superflues, les organisations peuvent se concentrer sur la sécurisation des fonctions qui sont requises et sur la réduction du risque que des fonctions inconnues soient exploitées.</p> <p>Inclure ces normes et ces processus renforçant les serveurs répond aux implications de sécurité spécifiques associées avec les fonctions superflues (par exemple, avec la suppression/désactivation de la fonction FTP ou du serveur Web si celui-ci n'exécute pas ces fonctions).</p>
<p>2.3 Crypter tous les accès administratifs non console, à l'aide d'une cryptographie robuste.</p> <p><i>Remarque : Les conditions dans l'annexe A2 doivent être remplies avec l'utilisation du SSL/TLS initial.</i></p>	<p>2.3 Sélectionner un échantillon de composants de système et vérifier l'accès administratif non-console est crypté en suivant la procédure ci-après :</p> <p>2.3.a Observer un administrateur se connecter à chaque système et examiner les configurations de système pour vérifier qu'une méthode de cryptage robuste est appelée avant que l'administrateur ne soit invité à taper son mot de passe.</p> <p>2.3.b Examiner les services et les fichiers de paramètre sur le système pour déterminer que Telnet et d'autres commandes de connexion à distance non sécurisées ne</p>	<p>Si l'administration non console (y compris l'administration à distance) ne s'effectue pas par le biais d'une authentification sécurisée et de communications cryptées, les informations administratives ou de niveau opérationnel sensibles (comme les mots de passe de l'administrateur) peuvent être interceptées. Un individu malveillant pourrait utiliser ces informations pour accéder au réseau, se substituer à l'administrateur et subtiliser des données.</p> <p>Les protocoles en texte clair (tels que HTTP, telnet, etc.) ne cryptent pas les détails de trafic ou de</p>

Conditions PCI DSS	Procédures de test	Directive
	sont pas disponibles pour l'accès non console.	<p>connexion, il est donc plus facile pour une personne malveillante d'intercepter cette information.</p> <p style="text-align: right;"><i>(suite à la page suivante)</i></p>
	<p>2.3.c Observer un administrateur se connecter à chaque système pour vérifier que l'accès administrateur aux interfaces de gestion Web est crypté au moyen d'une méthode de cryptage robuste.</p> <p>2.3.d Examiner la documentation du fournisseur et interroger le personnel pour vérifier qu'une cryptographie robuste est implémentée pour la technologie utilisée, conformément aux meilleures pratiques du secteur et/ou aux recommandations du fournisseur.</p> <p>2.3.e En cas d'utilisation du SSL/TLS initial, suivre les procédures de test dans <i>l'Annexe A2 : Autres conditions de la norme PCI DSS s'appliquant aux entités qui utilisent le SSL/TLS initial.</i></p>	<p>Pour être considérés comme une « cryptographie robuste », des protocoles reconnus par le secteur avec des clés robustes et une gestion de clé appropriée doivent être mis en place et être applicable pour le type de technologie utilisée. (Se rapporter à « Cryptographie robuste » dans le <i>Glossaire des termes, abréviations et acronymes PCI DSS et PA-DSS</i> et aux normes sectorielles et meilleures pratiques, comme NIST SP 800-52 et SP 800-57, OWASP, etc.)</p>
<p>2.4 Maintenir un inventaire des composants de système qui se trouvent dans le champ d'application de la norme PCI DSS.</p>	<p>2.4.a Examiner l'inventaire de système pour vérifier qu'une liste de composants de logiciel et de matériel est maintenue et comprend une description de la fonction/utilisation de chacun de ces composants.</p> <p>2.4.b Interroger le personnel pour vérifier que l'inventaire documenté est tenu à jour.</p>	<p>Maintenir une liste actualisée de tous les composants de système permettra à une organisation de définir précisément et efficacement la portée de son environnement pour l'implémentation des contrôles PCI DSS. Sans inventaire, certains composants de système pourraient être oubliés et être exclus par inadvertance des normes de configuration de l'organisation.</p>
<p>2.5 Assurer que les politiques de sécurité et les procédures opérationnelles pour la gestion des paramètres par défaut du fournisseur et des autres paramètres de sécurité sont documentés, utilisés et connus de toutes les parties concernées.</p>	<p>2.5 Examiner la documentation et interroger le personnel pour vérifier que les politiques de sécurité et les procédures opérationnelles pour la gestion des paramètres par défaut du fournisseur et des autres paramètres de sécurité sont :</p> <ul style="list-style-type: none"> • Documentées, • Utilisées et • Connues de toutes les parties concernées. 	<p>Le personnel doit être conscient et suivre les politiques de sécurité et les procédures opérationnelles quotidiennes pour assurer que les paramètres par défaut du fournisseur et les autres paramètres de sécurité sont continuellement gérés pour empêcher les configurations non sécurisées.</p>

Conditions PCI DSS	Procédures de test	Directive
<p>2.6 Les fournisseurs d'hébergement partagé doivent protéger l'environnement hébergé et les données de titulaires de carte de chaque entité. Ces fournisseurs doivent satisfaire aux conditions spécifiques décrites dans l'<i>Annexe A1 : Autres clauses de la norme PCI DSS s'appliquant aux fournisseurs d'hébergement partagé</i>.</p>	<p>2.6 Exécuter les procédures de test A.1.1 à A.1.4 décrites dans l'<i>Annexe A1 : Autres conditions de la norme PCI DSS s'appliquant aux fournisseurs d'hébergement partagé</i> pour l'évaluation PCI DSS des fournisseurs d'hébergement partagé, afin de vérifier que les fournisseurs d'hébergement partagé protègent l'environnement hébergé et les données de leurs entités (commerçants et prestataires de services).</p>	<p>Ceci est destiné aux fournisseurs d'hébergement qui proposent des environnements d'hébergement partagé à des clients multiples sur le même serveur. Lorsque les données sont sur le même serveur et sous contrôle d'un seul environnement, souvent les réglages de ces serveurs partagés ne sont pas réglables par les clients individuels. Cela permet aux clients d'ajouter des fonctions et des scripts non sécurisés susceptibles d'affecter la sécurité des environnements de tous les autres clients et, par conséquent, permettent à un individu malveillant de compromettre les données d'un client, et par là, d'accéder à toutes les données des autres clients. Voir l'<i>Annexe A1</i> pour plus de détails sur les conditions.</p>

Protection des données de titulaires de carte

Condition 3 : Protéger les données de titulaires de carte stockées

Les méthodes de protection, comme le cryptage, la troncature, le masquage et le hachage, sont des composants stratégiques de la protection des données de titulaires de carte. Si un intrus parvient à contourner les autres contrôles de sécurité et à accéder aux données cryptées, il ne pourra pas les lire ni les utiliser s'il n'a pas les clés cryptographiques appropriées. D'autres méthodes efficaces de protection des données stockées doivent aussi être envisagées pour potentiellement limiter les risques. Par exemple, pour minimiser les risques, éviter de stocker les données de titulaires de carte à moins que cela ne soit absolument nécessaire, tronquer les données de titulaires de carte si un PAN complet n'est pas requis et éviter d'envoyer un PAN non protégé par les technologies pour utilisateur final, comme les e-mails ou les messageries instantanées.

Pour obtenir la définition d'une « cryptographie robuste » et d'autres termes relatifs à PCI DSS, consulter le *Glossaire des termes, abréviations et acronymes PCI DSS*.

Conditions PCI DSS	Procédures de test	Directive
<p>3.1 Garder le stockage de données de titulaires de carte à un niveau minimum en appliquant des politiques, procédures et processus de conservation et d'élimination des données, qui comprennent au moins les mesures suivantes pour le stockage des données de titulaires de carte (CHD) :</p> <ul style="list-style-type: none"> • Limiter la quantité des données stockées et les délais de conservation selon les conditions requises par les conditions légales, réglementaires et/ou commerciales • Des conditions de conservation spécifiques pour les données de titulaires de carte ; • Des processus pour la suppression sécurisée des données devenues inutiles ; 	<p>3.1.a Examiner les politiques, procédures et processus de conservation et d'élimination des données pour vérifier qu'ils comprennent les points suivants pour le stockage de toutes les données de titulaires de carte :</p> <ul style="list-style-type: none"> • Limiter la quantité des données stockées et les délais de conservation selon les conditions requises par les conditions légales, réglementaires et/ou commerciales. • Des conditions spécifiques de conservation des données de titulaires de carte (par exemple, ces données doivent être conservées pendant une période X pour des raisons professionnelles Y) ; • Traiter la suppression sécurisée des données de titulaires de carte lorsque ces dernières ne sont plus requises pour des raisons légales, réglementaires ou commerciales. • Un processus trimestriel pour l'identification et la suppression sécurisée des données de titulaires de carte stockées excédant les conditions de conservation définies. 	<p>Une politique officielle de conservation des données identifie les données qui doivent être conservées, leur lieu de conservation afin de pouvoir les détruire en toute sécurité dès qu'elles ne sont plus nécessaires.</p> <p>Les seules données de titulaires de carte à stocker après autorisation sont le numéro de compte primaire ou PAN (rendu illisible), la date d'expiration, le nom du titulaire de la carte et le code de service.</p> <p>Comprendre où les données de titulaires de carte sont situées est nécessaire pour que ces données puissent être conservées ou éliminées lorsqu'elles ne sont plus nécessaires. Afin de définir les conditions appropriées de conservation, une entreprise doit d'abord comprendre les besoins de son activité ainsi que les obligations légales et réglementaires qui</p>

Conditions PCI DSS	Procédures de test	Directive
<ul style="list-style-type: none"> Un processus trimestriel pour l'identification et la suppression sécurisée des données de titulaires de carte stockées excédant les conditions de conservation définies. 	<p>3.1.c Interroger le personnel pour vérifier que :</p> <ul style="list-style-type: none"> Tous les emplacements où des données de titulaires de carte sont stockées sont inclus dans les processus de rétention et d'élimination. Un processus trimestriel automatique ou manuel est en place pour l'identification et la suppression sécurisée des données de titulaires de carte stockées. Le processus trimestriel automatique ou manuel est effectué sur tous les emplacements de données de titulaires de carte. 	<p>s'appliquent à son secteur et/ou au type de données conservées.</p> <p style="text-align: right;"><i>(suite à la page suivante)</i></p>
	<p>3.1.c Pour un échantillon des composants de système qui stockent les données de titulaires de carte :</p> <ul style="list-style-type: none"> Examiner les archives de fichiers et de système pour vérifier que les données stockées n'excèdent pas les conditions définies dans la politique de conservation des données. Observer le mécanisme d'élimination pour vérifier que les données sont éliminées de manière sécurisée. 	<p>L'identification et la suppression des données stockées qui ont dépassé la période de rétention spécifiée empêche la rétention de données qui ne sont plus utiles. Ce processus peut être automatique ou manuel, ou une combinaison des deux. Par exemple, une procédure de programmation (automatique ou manuelle) pour localiser et supprimer les données et/ou un examen manuel des zones de stockage de données pourraient être effectués.</p> <p>La mise en œuvre de méthodes de destruction sécurisées garantit que les données ne pourront pas être récupérées une fois qu'elles ne seront plus nécessaires.</p> <p><i>Il ne faut pas oublier qu'il est inutile de stocker ce dont on n'a pas besoin !</i></p>
<p>3.2 Ne stocker aucune donnée d'identification sensible après autorisation (même cryptée). Si des données d'identification sensibles sont reçues, rendre toutes les données irrécupérables à la fin du processus d'autorisation.</p> <p><i>Il est permis aux émetteurs et aux sociétés qui prennent en charge les services</i></p>	<p>3.2.a Pour les émetteurs et/ou sociétés qui prennent en charge les services d'émission et stockent des données d'identification sensibles, examiner les politiques et interroger le personnel pour vérifier qu'il y a une justification commerciale documentée pour le stockage des données d'identification sensibles.</p>	<p>Les données d'identification sensibles sont constituées par les données complètes de piste, le code ou la valeur de validation de carte et les données PIN. Le stockage des données d'identification sensibles n'est pas autorisé ! Ces données sont précieuses pour les individus malveillants, car elles leur permettent de créer de fausses cartes de paiement et de procéder à des transactions frauduleuses.</p>

Conditions PCI DSS	Procédures de test	Directive
<p><i>d'émissions de stocker des données d'identification sensibles si :</i></p> <ul style="list-style-type: none"> • Une justification commerciale existe et • Les données sont stockées de manière sécurisée <p>Les données d'identification sensibles sont mentionnées dans les conditions 3.2.1 à 3.2.3 suivantes :</p>	<p>3.2.b Pour les émetteurs et/ou les sociétés qui prennent en charge les services d'émission et stockent des données d'identification sensibles, examiner les stockages de données et les configurations de système pour vérifier que les données d'identification sensibles sont sécurisées.</p>	<p>Les entités qui émettent des cartes de paiement ou qui fournissent ou soutiennent des services d'émission créeront et contrôleront souvent des données d'identification sensibles dans le cadre de la fonction d'émission. Les entreprises peuvent exécuter, permettre ou prendre en charge des services de stockage des données d'identification sensibles UNIQUEMENT SI elles en ont un besoin professionnel légitime.</p> <p>Il faut remarquer que l'ensemble des conditions de la norme PCI DSS s'applique aux émetteurs et que la seule exception les concernant, ainsi que leurs processeurs, est que les données d'identification sensibles peuvent être conservées s'il existe une raison légitime pour ce faire. Une raison légitime est une raison nécessaire pour l'accomplissement de la fonction fournie pour l'émetteur, et non une raison de pure convenance. Ces données doivent être stockées en sécurité, conformément à toutes les conditions de la norme PCI DSS et à aux conditions spécifiques de la marque de carte de paiement.</p>
	<p>3.2.c Pour toutes les autres entités, si des données d'identification sensibles sont reçues, examiner les politiques et procédures et examiner les configurations de système pour vérifier que les données ne sont pas conservées après autorisation.</p>	
	<p>3.2.b Pour toutes les autres entités, si des données d'identification sensibles sont reçues, examiner les procédures et les processus d'élimination sécurisée des données pour vérifier que les données ne sont pas récupérables.</p>	<p>Pour les entités non émettrices qui conservent des données d'identification sensibles, la post-autorisation n'est pas permise.</p>

Conditions PCI DSS	Procédures de test	Directive
<p>3.2.1 Ne pas stocker la totalité du contenu d'une quelconque piste (sur la bande magnétique au verso d'une carte, sur une puce ou ailleurs) après l'autorisation. Ces données sont également désignées piste complète, piste, piste 1, piste 2 et données de bande magnétique.</p> <p>Remarque : Dans le cadre normal de l'activité, il est parfois nécessaire de conserver les éléments de données de la bande magnétique suivants :</p> <ul style="list-style-type: none"> • Le nom du titulaire de la carte • Le numéro de compte primaire (PAN) ; • La date d'expiration ; • Le code de service <p>Afin de réduire le risque autant que possible, stocker uniquement les éléments de données nécessaires à l'activité.</p>	<p>3.2.1 Sur un échantillon de composants de système, examiner les sources de données, y compris sans s'y limiter les éléments suivants, et vérifier que la totalité du contenu d'une quelconque piste de la bande magnétique au verso d'une carte ou sur une puce, ou donnée équivalente sur une puce, n'est en aucun cas stockée après autorisation :</p> <ul style="list-style-type: none"> • Les données de transaction entrantes ; • Tous les journaux (par exemple, transactions, historique, débogage, erreur) ; • Les fichiers d'historique • Les fichiers trace • Plusieurs schémas de bases de données ; • Contenu des bases de données. 	<p>Si les données complètes de piste étaient stockées, les individus malveillants qui obtiennent ces données pourraient les utiliser pour reproduire et vendre des cartes de paiement pour effectuer des transactions frauduleuses.</p>
<p>3.2.2 Ne pas stocker le code ou la valeur de vérification de carte (nombre à trois ou quatre chiffres figurant au recto ou au verso de la carte de paiement, utilisé pour vérifier les transactions carte absente) après l'autorisation.</p>	<p>3.2.2 Sur un échantillon de composants de système, examiner les sources de données, y compris sans s'y limiter les éléments suivants, et vérifier que le code ou la valeur de vérification de carte à trois ou quatre chiffres figurant au recto de la carte de paiement, ou dans l'espace réservé à la signature (données CVV2, CVC2, CID, CAV2) n'est en aucun cas stocké après autorisation :</p> <ul style="list-style-type: none"> • Les données de transaction entrantes ; • Tous les journaux (par exemple, transactions, historique, débogage, erreur) ; • Les fichiers d'historique • Les fichiers trace • Plusieurs schémas de bases de données ; • Contenu des bases de données. 	<p>Le code de validation des cartes est destiné à protéger les transactions « carte absente », transactions effectuées via Internet ou ordre de paiement par e-mail/téléphone (MOTO), en l'absence du consommateur et de la carte.</p> <p>Si ces données étaient volées, des individus malveillants pourraient exécuter des transactions frauduleuses par MO/TO et Internet.</p>

Conditions PCI DSS	Procédures de test	Directive
<p>3.2.3 Ne pas stocker de code d'identification personnelle (PIN) ou de bloc PIN crypté après l'autorisation.</p>	<p>3.2.3 Sur un échantillon de composants de système, examiner les sources de données, y compris sans s'y limiter les éléments suivants, et vérifier que les codes et blocs PIN cryptés ne sont pas stockés après autorisation :</p> <ul style="list-style-type: none"> • Les données de transaction entrantes ; • Tous les journaux (par exemple, transactions, historique, débogage, erreur) ; • Les fichiers d'historique • Les fichiers trace • Plusieurs schémas de bases de données ; • Contenu des bases de données. 	<p>Ces valeurs ne doivent être connues que du titulaire de la carte ou de la banque émettrice de la carte. Si ces données étaient volées, des individus malveillants pourraient exécuter des transactions de débit frauduleuses à l'aide du code PIN (par exemple, retraits à un GAB).</p>
<p>3.3 Masquer le PAN lorsqu'il s'affiche (les six premiers chiffres et les quatre derniers sont le maximum de chiffres affichés), de manière à ce que seul le personnel, dont le besoin commercial est légitime, puisse voir plus que les six premiers/les quatre derniers chiffres du PAN.</p> <p>Remarque : Cette condition ne se substitue pas aux conditions plus strictes qui sont en place et qui régissent l'affichage des données de titulaires de carte, par exemple, pour les reçus des points de vente (POS).</p>	<p>3.3.a Examiner les politiques et les procédures écrites de masquage de l'affichage de PAN pour vérifier que :</p> <ul style="list-style-type: none"> • Une liste des rôles qui ont besoin d'accéder aux affichages contenant plus que les six premiers/quatre derniers chiffres (PAN entier) est documentée, ainsi que le besoin commercial légitime de chaque rôle pour cet accès. • Le PAN doit être masqué de sorte que seul le personnel qui a un besoin professionnel légitime puisse voir plus que les six premiers/les quatre derniers chiffres du PAN. • Tous les rôles qui ne sont pas spécifiquement autorisés à voir le PAN entier doivent uniquement voir des PAN masqués. <p>3.3.b Examiner les configurations de système pour vérifier que le PAN entier est uniquement affiché pour les utilisateurs/rôles ayant un besoin commercial documenté et que le PAN est masqué pour toutes les autres demandes.</p>	<p>Grâce à l'affichage du PAN intégral sur un écran d'ordinateur, un reçu de carte de paiement, un fax ou un rapport sur papier, des individus non autorisés pourraient y avoir accès et l'utiliser de manière frauduleuse. Assurer que le PAN est uniquement affiché pour les personnes ayant un besoin commercial légitime de le voir minimise les risques de personnes non autorisées obtenant accès aux données de PAN.</p> <p>Le masquage doit toujours s'assurer que seul le nombre minimal nécessaire de chiffres s'affiche pour exécuter une fonction professionnelle spécifique. Par exemple, si seuls les quatre derniers chiffres sont requis pour exécuter une fonction professionnelle, masquez le PAN afin que les individus chargés de cette fonction puissent afficher uniquement les quatre derniers</p>

Conditions PCI DSS	Procédures de test	Directive
	<p>3.3.c Examiner l’affichage du PAN (par exemple, à l’écran, sur les reçus papier) afin de vérifier que le PAN est masqué lors de l’affichage des données de titulaires de carte, sauf pour les utilisateurs qui ont un besoin professionnel légitime de voir plus que les six premiers/les quatre derniers chiffres du PAN.</p>	<p>chiffres. En outre, si une fonction doit accéder au numéro d’identification bancaire (BIN) dans un souci d’acheminement, démasquer les chiffres BIN uniquement (habituellement les six premiers chiffres) pendant l’exécution de cette fonction.</p> <p>Cette condition porte sur la protection du PAN <u>visible</u> sur les écrans, reçus papier, impressions, etc. et elle ne doit pas être confondue avec la condition 3.4 de protection du PAN lorsqu’il est <u>stocké</u> dans des fichiers, des bases de données, etc.</p>

Conditions PCI DSS	Procédures de test	Directive
<p>3.4 Rendre le PAN illisible où qu'il soit stocké (y compris les données sur support numérique portable, support de sauvegarde et journaux), en utilisant l'une des approches suivantes :</p> <ul style="list-style-type: none"> • Hachage unilatéral s'appuyant sur une méthode cryptographique robuste (la totalité du PAN doit être hachée) ; • Troncature (le hachage ne peut pas être utilisé pour remplacer le segment tronqué du PAN) ; • Jetons et pads d'index (les pads doivent être stockés de manière sécurisée) ; • Cryptographie robuste associée aux processus et procédures de gestion des clés. <p>Remarque : Il s'agit d'un effort relativement peu important pour un individu malveillant de reconstruire les données du PAN d'origine, s'il a à la fois accès à la version tronquée et hachée d'un PAN. Lorsque les versions hachées et tronquées du même</p>	<p>3.4.a Examiner la documentation relative au système utilisé pour protéger le PAN, notamment le fournisseur, le type de système/processus et les algorithmes de cryptage (le cas échéant) pour vérifier que le PAN est rendu illisible en utilisant l'une des méthodes suivantes :</p> <ul style="list-style-type: none"> • Hachage unilatéral s'appuyant sur une méthode cryptographique robuste, • Troncature ; • Jetons et pads d'index, les pads devant être stockés de manière sécurisée ; • Cryptographie robuste associée aux processus et procédures de gestion des clés. <p>3.4.b Examiner plusieurs tables ou fichiers d'un échantillon de référentiels de données afin de vérifier que le PAN est rendu illisible (en d'autres termes, qu'il n'est pas stocké en texte clair).</p> <p>3.4.c Examiner un échantillon de support amovible (par exemple, bandes de sauvegarde) pour s'assurer que le PAN est rendu illisible.</p> <p>3.4.d Examiner un échantillon de journaux d'audit, y compris les journaux d'application de paiement, pour confirmer que le PAN est bien illisible ou supprimé des journaux.</p>	<p>Les PAN stockés sur les supports de stockage principal (bases de données ou fichiers plats comme les feuilles de calcul) et autres supports secondaires (sauvegardes ou journaux d'audit, d'anomalies ou de dépannage) doivent tous être protégés.</p> <p>Les fonctions de hachage unilatéral reposant sur une cryptographie robuste peuvent être utilisées pour rendre les données de titulaires de carte illisibles. Ces fonctions de hachage sont appropriées lorsqu'il n'est pas nécessaire de récupérer le numéro d'origine (le hachage unilatéral est irréversible). Il est recommandé, bien que ce ne soit pas une condition, qu'une valeur supplémentaire aléatoire soit ajoutée aux données de titulaires de carte avant le hachage pour réduire la possibilité qu'un pirate puisse comparer les données (et découvrir le PAN) à des tableaux de valeurs de hachage pré-calculées.</p> <p>L'objectif d'une troncature consiste à supprimer définitivement un segment des données du PAN. Ainsi, seule une portion du PAN est stockée (généralement sans dépasser les six premiers et</p>

Conditions PCI DSS	Procédures de test	Directive
<p><i>PAN sont présentes dans l'environnement d'une entité, des contrôles supplémentaires doivent être en place pour garantir que les versions hachées et tronquées ne peuvent pas être corrélées pour reconstituer le PAN d'origine.</i></p>	<p>3.4.e Si les versions hachées et tronquées du même PAN sont présentes dans l'environnement, examiner les contrôles en place pour vérifier que les versions hachées et tronquées ne peuvent pas être corrélées pour reconstituer le PAN d'origine.</p>	<p>les quatre derniers chiffres).</p> <p>Un « jeton d'index » est un élément cryptographique qui remplace le PAN en fonction d'un indice donné, par une valeur imprévisible. Un pad ponctuel est un système dans lequel une clé privée, générée de façon aléatoire, est utilisée une seule fois pour crypter un message, qui est ensuite décrypté à l'aide de la clé et du pad ponctuel correspondant.</p> <p>L'objectif de la cryptographie robuste (selon la définition du <i>Glossaire des termes, abréviations et acronymes PCI DSS et PA-DSS</i>) est de fonder le cryptage sur un algorithme testé et accepté par le secteur (non pas un algorithme exclusif ou « développé en interne »), avec de robustes clés cryptographiques.</p> <p>En corrélant les versions hachées et tronquées d'un PAN donné, un individu malveillant peut facilement reconstituer le PAN d'origine. Des contrôles empêchant la corrélation de ces données permettront de garantir que le PAN d'origine reste illisible.</p>
<p>3.4.1 Si un cryptage par disque est utilisé (au lieu d'un cryptage de base de données au niveau fichier ou colonne), l'accès logique doit être géré séparément et indépendamment des mécanismes de contrôle d'accès au système d'exploitation natif (par exemple, en n'utilisant pas des bases de données de comptes d'utilisateur locales, ou des justificatifs génériques de connexion au réseau). Les clés de décryptage ne doivent pas être associées à des comptes</p>	<p>3.4.1.a Si un cryptage par disque est utilisé, inspecter la configuration et le processus d'authentification pour vérifier que l'accès logique aux systèmes de fichiers cryptés est implémenté par le biais d'un mécanisme indépendant des mécanismes des systèmes d'exploitation natifs (par exemple, en n'utilisant pas des bases de données de comptes d'utilisateur locales ou des justificatifs génériques de connexion au réseau).</p> <p>3.4.1.b Examiner les processus et interroger le personnel pour vérifier que les clés cryptographiques sont stockées de manière sécurisée (par exemple, sur des supports amovibles correctement protégés avec des contrôles d'accès stricts).</p>	<p>Le but de cette condition est d'adresser l'acceptabilité du cryptage par disque pour rendre les données de titulaires de carte illisibles. Le cryptage par disque crypte la totalité du disque/de la partition sur un ordinateur et décrypte automatiquement les informations à la demande d'un utilisateur autorisé. De nombreuses solutions de cryptage par disque interceptent les opérations de lecture et d'écriture du système d'exploitation et exécutent les transformations cryptographiques appropriées sans autre action particulière de l'utilisateur que la saisie d'un mot de passe ou phrase au démarrage du système ou au début</p>

Conditions PCI DSS	Procédures de test	Directive
<p>d'utilisateur.</p> <p>Remarque : En outre, cette condition s'applique à toutes les autres conditions de gestion des clés et de cryptage PCI DSS.</p>	<p>3.4.1.c Examiner les configurations et observer les processus pour vérifier que les données de titulaires de carte sur les supports amovibles sont cryptées où qu'elles soient stockées.</p> <p>Remarque : Si le cryptage de disque n'est pas utilisé pour crypter les supports amovibles, les données stockées sur ce support devront être rendues illisibles par une autre méthode.</p>	<p>d'une session. Compte tenu de ces caractéristiques du cryptage par disque, pour être conforme à cette condition, la méthode ne peut pas :</p> <ol style="list-style-type: none"> 1) Utiliser le même authentifiant de compte utilisateur que le système d'exploitation, ou 2) Utiliser une clé de décryptage qui est associée ou dérivée de la base de données du compte d'utilisateur local de système ou des justificatifs génériques de connexion au réseau. <p>Le cryptage total par disque aide à protéger les données en cas de perte physique d'un disque et il peut donc convenir aux périphériques portables qui stockent les données de titulaires de carte.</p>
<p>3.5 Documenter et mettre en œuvre des procédures pour protéger les clés utilisées pour sécuriser les données de titulaires de carte stockées contre la divulgation et l'utilisation illicites :</p> <p>Remarque : Cette condition s'applique également aux clés utilisées pour crypter les données de titulaires de carte stockées et elle s'applique aux clés de cryptage de clé utilisées pour protéger les clés de cryptage de données – ces clés de cryptage de données doivent être au moins aussi robustes que la clé de cryptage de données.</p>	<p>3.5 Vérifier les politiques et procédures de gestion des clés pour vérifier que des processus sont spécifiés pour protéger les clés utilisées pour le cryptage des données de titulaires de carte contre la divulgation et l'utilisation illicite en procédant comme suit :</p> <ul style="list-style-type: none"> • L'accès aux clés cryptographiques est restreint au plus petit nombre d'opérateurs possible. • Les clés de cryptage de clés sont au moins aussi robustes que les clés de cryptage de données qu'elles protègent. • Les clés de cryptage de clés sont stockées à un emplacement différent des clés de cryptage de données. • Les clés sont stockées de manière sécurisée dans aussi peu d'emplacements et sous aussi peu de formes que possible. 	<p>Les clés cryptographiques doivent être parfaitement bien protégées, car tout individu qui parviendrait à y accéder pourrait décrypter les données. Les clés de cryptage de clés, si elles sont utilisées, doivent au moins être aussi robustes que les clés de cryptage de données afin de garantir une protection adéquate de la clé qui crypte les données aussi bien que des données cryptées à l'aide de la clé.</p> <p>L'obligation de protéger les clés d'une divulgation et d'une utilisation illicites s'applique aux clés de cryptage des données comme à celles assurant le cryptage des clés. Une seule clé de cryptage de clé pouvant permettre d'accéder à de nombreuses clés de cryptage de données, il est nécessaire d'appliquer des mesures robustes pour protéger les clés de cryptage de clés.</p>

Conditions PCI DSS	Procédures de test	Directive
<p>3.5.1 Conditions supplémentaires pour les prestataires de services uniquement : Conserver une description documentée de l'architecture cryptographique qui comprend ce qui suit :</p> <ul style="list-style-type: none"> Détails de tous les algorithmes, protocoles et clés utilisés pour protéger les données de titulaires de carte, y compris la robustesse des clés et la date d'expiration Description de l'utilisation de chaque clé Inventaire des HSM et autres SCD dans le cadre de la gestion des clés <p><i>Remarque</i> : Cette condition est considérée comme une meilleure pratique jusqu'au 31 janvier 2018, après quoi ce sera une obligation.</p>	<p>3.5.1 Interroger le personnel responsable et examiner la documentation pour vérifier qu'un document existe pour décrire l'architecture cryptographique, y compris :</p> <ul style="list-style-type: none"> Détails de tous les algorithmes, protocoles et clés utilisés pour protéger les données de titulaires de carte, y compris la robustesse des clés et la date d'expiration Description de l'utilisation de chaque clé Inventaire des HSM et autres SCD dans le cadre de la gestion des clés 	<p><i>Remarque</i> : Cette condition ne s'applique que lorsque l'entité évaluée est un prestataire de services.</p> <p>La conservation de la documentation actuelle de l'architecture cryptographique permet à une entité de comprendre les algorithmes, les protocoles et les clés cryptographiques utilisés pour protéger les données de titulaires de carte, et les appareils qui génèrent, utilisent et protègent les clés. Ainsi, une entité peut adapter son architecture face aux menaces en constante évolution et planifier des mises à jour au fur et à mesure des changements apportés aux niveaux d'assurance fournis par les diverses robustesses d'algorithmes/de clés. La gestion d'une telle documentation permet aussi à une entité de détecter les clés perdues ou manquantes ou les appareils de gestion des clés et d'identifier les ajouts non autorisés dans son architecture cryptographique.</p>
<p>3.5.2 Restreindre l'accès aux clés cryptographiques au plus petit nombre d'opérateurs possible.</p>	<p>3.5.2 Examiner les listes d'accès utilisateur afin de vérifier que l'accès aux clés est restreint aux opérateurs strictement nécessaires.</p>	<p>Seul un petit nombre de personnes doit avoir accès aux clés cryptographiques (pour réduire le potentiel de rendre les données de titulaires de carte visibles pour des parties non autorisées), en général ceux qui sont chargés de la gestion de ces clés.</p>

Conditions PCI DSS	Procédures de test	Directive
<p>3.5.3 Stocker les clés secrètes et privées utilisées pour crypter/décrypter les données de titulaires de carte sous l'une (ou sous plusieurs) des formes suivantes à tout moment :</p> <ul style="list-style-type: none"> • Cryptées avec une clé de cryptage de clé qui est au moins aussi robuste que la clé de cryptage de données et qui est stocké séparément de la clé de cryptage de données. • Dans un périphérique cryptographique sécurisé (comme un module de sécurité matériel (hôte) ou un dispositif de point d'interaction approuvé PTS) • En tant que deux composants de clé ou partages de clé de pleine longueur au moins, conformément à la méthode acceptée par l'industrie <p>Remarque : <i>Il n'est pas nécessaire que les clés publiques soient stockées sous l'une de ces formes.</i></p>	<p>3.5.3.a Examiner les procédures documentées pour vérifier que les clés cryptographiques utilisées pour crypter/décrypter les données de titulaires de carte doivent uniquement exister sous l'une (ou sous plusieurs) des formes suivantes à tout moment :</p> <ul style="list-style-type: none"> • Cryptées avec une clé de cryptage de clé qui est au moins aussi robuste que la clé de cryptage de données et qui est stockée séparément de la clé de cryptage de données. • Dans un périphérique cryptographique sécurisé (comme un module de sécurité matériel (hôte) ou un dispositif de point d'interaction approuvé PTS) • En tant que deux composants de clé ou partages de clé conformément à la méthode acceptée par l'industrie <p>3.5.3.b Examiner les configurations du système et les emplacements de stockage de clés pour vérifier que les clés cryptographiques utilisées pour crypter/décrypter les données de titulaires de carte existent toujours sous l'une (ou sous plusieurs) des formes suivantes :</p> <ul style="list-style-type: none"> • Cryptées avec une clé de cryptage de clé • Dans un périphérique cryptographique sécurisé (comme un module de sécurité matériel (hôte) ou un dispositif de point d'interaction approuvé PTS) • En tant que deux composants de clé ou partages de clé conformément à la méthode acceptée par l'industrie <p>3.5.3.c Lorsque des clés de cryptage de clé sont utilisées, examiner les configurations du système et les emplacements de stockage de clé pour vérifier que :</p> <ul style="list-style-type: none"> • Les clés de cryptage de clés sont au moins aussi robustes que les clés de cryptage de données qu'elles protègent. • Les clés de cryptage de clés sont stockées à un emplacement différent des clés de cryptage de données. 	<p>Les clés cryptographiques doivent être stockées de manière sécurisée pour prévenir des accès non autorisés ou inutiles qui pourraient provoquer l'exposition des données de titulaires de carte.</p> <p>Il n'est pas prévu de crypter les clés de cryptage de clés, mais celles-ci doivent cependant être protégées de la divulgation et de l'utilisation illicites comme le définit la condition 3.5 Si des clés de cryptage de clé sont utilisées, le stockage des clés de cryptage des clés dans des endroits matériels et/ou logiciels distincts de ceux des clés de cryptage de données réduit le risque d'accès non autorisé à ces deux types de clés.</p>

Conditions PCI DSS	Procédures de test	Directive
<p>3.5.4 Stocker les clés cryptographiques dans aussi peu d'emplacements que possible.</p>	<p>3.5.4 Examiner les emplacements de stockage de clé et observer les processus pour vérifier que les clés sont stockées dans aussi peu d'endroits que possible.</p>	<p>Le stockage des clés cryptographiques dans le moins d'endroits possibles aide une organisation à suivre et à surveiller tous les emplacements de clés et à minimiser le potentiel que les clés soient exposées à des parties non autorisées.</p>
<p>3.6 Documenter en détail et déployer les processus et les procédures de gestion des clés cryptographiques servant au cryptage des données de titulaires de carte, notamment ce qui suit :</p> <p>Remarque : De nombreuses normes du secteur pour la gestion des clés sont disponibles auprès de diverses ressources, notamment NIST, que vous trouverez à l'adresse suivante : http://csrc.nist.gov.</p>	<p>3.6.a Procédure de tests supplémentaires pour évaluer les prestataires de services uniquement : Si le prestataire de services partage des clés avec ses clients pour la transmission ou le stockage de données de titulaires de carte, examiner la documentation apportée par le prestataire de service à ses clients pour vérifier qu'elle comprend les instructions sur la manière de sécuriser la transmission, le stockage et la mise à jour des clés conformément aux conditions 3.6.1 à 3.6.8 ci-dessous.</p> <p>3.6.b Examiner les procédures et les processus de gestion de clé utilisée pour le cryptage des données de titulaires de carte et effectuer ce qui suit :</p>	<p>La manière dont les clés cryptographiques sont gérées est un aspect essentiel de la sécurité permanente de la solution de cryptage. Un bon processus de gestion des clés, qu'il soit manuel ou automatique, dans le cadre du produit de cryptage, se base sur les normes du secteur et prend en charge tous les éléments essentiels décrits aux points 3.6.1 à 3.6.8.</p> <p>Donner des directives aux clients sur la manière de transmettre, stocker et mettre à jour les clés cryptographiques de manière sécurisée peut aider à empêcher que les clés soient mal gérées ou communiquées à des entités non autorisées.</p> <p>Cette condition s'applique aux clés utilisées pour crypter les données de titulaires de carte stockées ainsi qu'à toute clé de cryptage de clé associée.</p> <p>Remarque : La procédure de test 3.6.a est une procédure supplémentaire, qui s'applique uniquement si l'entité en cours d'évaluation est un prestataire de services.</p>
<p>3.6.1 Génération de clés cryptographiques robustes</p>	<p>3.6.1.a Vérifier que des procédures de gestion des clés spécifient comment générer des clés robustes.</p> <p>3.6.1.b Observer les procédures de génération des clés pour vérifier que des clés robustes sont générées.</p>	<p>La solution de cryptage doit générer des clés robustes, comme défini dans le <i>Glossaire des termes, abréviations et acronymes PCI DSS et PA-DSS</i> dans la section « Génération de clés cryptographiques ». L'utilisation de clés cryptographiques robustes augmente de manière significative le niveau de sécurité des données de titulaires de carte.</p>
<p>3.6.2 Sécuriser la distribution des clés cryptographiques</p>	<p>3.6.2.a Vérifier que des procédures de gestion des clés spécifient comment distribuer les clés de manière sécurisée.</p>	<p>La solution de cryptage doit distribuer les clés de manière sécurisée, c'est-à-dire que les clés sont</p>

Conditions PCI DSS	Procédures de test	Directive
	3.6.2.b Observer la méthode de distribution des clés pour vérifier que les clés sont distribuées de manière sécurisée.	uniquement distribuées aux individus chargés de leur gestion identifiés au point 3.5.1 et qu'elles ne sont jamais distribuées en texte clair.
3.6.3 Sécuriser le stockage des clés cryptographiques	3.6.3.a Vérifier que des procédures de gestion des clés spécifient comment stocker les clés de manière sécurisée. 3.6.3.b Observer la méthode de stockage de clé pour vérifier que les clés sont stockées de manière sécurisée.	La solution de cryptage doit stocker les clés de manière sécurisée, par exemple, en les cryptant à l'aide d'une clé de cryptage de clé. Le stockage des clés sans protection adéquate pourrait donner un accès aux pirates et provoquer le décryptage et l'exposition des données de titulaires de carte.
3.6.4 Changements de clé cryptographique pour les clés ayant atteint la fin de leur cryptopériode (par exemple, après la fin d'une période définie et/ou après la production d'une certaine quantité de cryptogrammes par une clé donnée), comme l'a défini le fournisseur de l'application associée ou le propriétaire de la clé, et selon les meilleures pratiques et directives du secteur (par exemple, la publication spéciale NIST 800-57).	3.6.4.a Vérifier que les procédures de gestion des clés comprennent une cryptopériode définie pour chaque type de clé en utilisation et définissent un processus de changement de clé à la fin de la ou les cryptopériodes définies. 3.6.4.b Interroger le personnel pour vérifier que les clés sont changées la fin de la ou des cryptopériodes définies.	<p>La cryptopériode est la période durant laquelle une clé cryptographique donnée peut être utilisée dans le but pour lequel elle est prévue. Les facteurs à prendre en compte pour définir la cryptopériode sont, sans s'y limiter, la complexité de l'algorithme sous-jacent, la taille ou la longueur de la clé, le risque de compromission de la clé, et la sensibilité des données cryptées.</p> <p>Il est impératif de changer les clés de cryptage une fois leur cryptopériode écoulee, afin de réduire le risque qu'un tiers se les procure et les utilise pour décrypter des données.</p>
3.6.5 Retrait ou remplacement des clés (par exemple, en les archivant, détruisant, et/ou en les révoquant), si nécessaire lorsque le degré d'intégrité d'une clé est affaibli (par exemple, départ d'un employé ayant connaissance du texte clair d'une clé) ou lorsque des clés sont susceptibles d'avoir été compromises. <i>Remarque : Si les clés cryptographiques retirées ou remplacées doivent être conservées, ces clés doivent être archivées de manière sécurisée (par exemple, en utilisant une clé de cryptage de clé). Les clés cryptographiques archivées doivent</i>	3.6.5.a Vérifier que des procédures de gestion des clés spécifient les processus pour les points suivants : <ul style="list-style-type: none"> • Le retrait ou le remplacement des clés lorsque l'intégrité de la clé a été affaibli ; • Le remplacement des clés compromises ou suspectées de l'être. • Toute clé retirée ou remplacée n'est pas utilisée pour les opérations de cryptages. 3.6.5.b Interroger le personnel pour vérifier que des procédures sont mises en œuvre : <ul style="list-style-type: none"> • Les clés sont retirées ou remplacées si nécessaire lorsque leur intégrité a été affaibli, y compris lorsque quelqu'un connaissant la clé quitte la société. 	<p>Les clés qui ne sont plus utilisées ou nécessaires, ou les clés dont on sait ou on soupçonne qu'elles sont compromises, doivent être révoquées et/ou détruites pour assurer qu'elles ne puissent plus être utilisées. Ces clés doivent être conservées (par exemple, pour prendre en charge des données cryptées archivées), elles doivent être parfaitement protégées.</p> <p>La solution de cryptage doit également permettre et faciliter un processus de remplacement des clés qui doivent être remplacées ou dont on sait, ou dont on soupçonne qu'elles sont compromises.</p>

Conditions PCI DSS	Procédures de test	Directive
<p><i>être utilisées uniquement pour un décryptage ou une vérification.</i></p>	<ul style="list-style-type: none"> • Les clés sont remplacées si on sait ou on soupçonne qu'elles sont compromises. • Toute clé conservée après son retrait ou son remplacement n'est pas utilisée pour les opérations de cryptages. 	
<p>3.6.6 Si des opérations de gestion manuelle de clés cryptographiques en texte clair sont utilisées, elles doivent être gérées par le fractionnement des connaissances et un double contrôle.</p> <p>Remarque : <i>La génération, la transmission, le chargement, le stockage et la destruction de clés sont quelques-uns des exemples d'interventions de gestion manuelle des clés.</i></p>	<p>3.6.6.a Vérifier que des procédures manuelles de gestion des clés en texte clair spécifient les processus d'utilisation de ce qui suit :</p> <ul style="list-style-type: none"> • Fractionnement des connaissances de clés, de sorte que les composants de clé sont sous le contrôle d'au moins deux personnes qui ne connaissent que leur propre composant de clé ET • Le double contrôle des clés, de sorte qu'au moins deux personnes doivent effectuer toutes les opérations de gestion de clé et qu'une seule personne ait accès au matériel d'authentification (par exemple les mots de passe ou les clés) d'une autre. <p>3.6.6.b Interroger le personnel et/ou observer les processus pour vérifier que les clés manuelles en texte clair sont gérées avec :</p> <ul style="list-style-type: none"> • Le fractionnement des connaissances ET • Le double contrôle 	<p>Le fractionnement des connaissances et le double contrôle des clés sont utilisés pour éliminer la possibilité qu'une seule personne puisse accéder à l'intégralité d'une clé. Ce contrôle s'applique aux opérations manuelles de cryptage des clés ou si la gestion des clés n'est pas prise en charge par la solution de cryptage.</p> <p>Le fractionnement des connaissances est une méthode par laquelle deux personnes ou plus détiennent séparément des composants clés ; chaque personne connaît uniquement son propre composant de clé et les composants de clé individuels ne contiennent aucune connaissance de la clé cryptographique d'origine.</p> <p>Le double contrôle demande que deux personnes ou plus effectuent une fonction et qu'une seule personne ne puisse pas accéder ou utiliser le matériel d'authentification d'une autre.</p>
<p>3.6.7 Prévention de la substitution non autorisée des clés cryptographiques.</p>	<p>3.6.7.a Vérifier que les procédures de gestion des clés spécifient les processus empêchant la substitution non autorisée des clés.</p> <p>3.6.7.b Interroger le personnel et/ou observer les processus pour vérifier que la substitution non autorisée des clés est empêchée.</p>	<p>La solution de cryptage ne doit pas autoriser ni accepter la substitution de clés de la part de sources non autorisées ou de processus inattendus.</p>
<p>3.6.8 Condition selon laquelle les opérateurs chargés de la gestion de clés cryptographiques reconnaissent formellement qu'ils comprennent et acceptent leurs responsabilités en tant</p>	<p>3.6.8.a Vérifier que les procédures de gestion des clés spécifient les processus selon lesquels les opérateurs chargés de la gestion de clés cryptographiques reconnaissent (par écrit ou électroniquement) qu'ils comprennent et acceptent leurs responsabilités en tant que telles.</p>	<p>Ce processus aidera à garantir que les individus chargés de la gestion des clés s'engagent vis-à-vis de leur rôle de détenteur de clé et qu'ils comprennent et acceptent leurs responsabilités.</p>

Conditions PCI DSS	Procédures de test	Directive
que telles.	<p>3.6.8.b Observer la documentation et les autres preuves montrant que les opérateurs chargés de la gestion de clés cryptographiques reconnaissent (par écrit ou électroniquement) qu'ils comprennent et acceptent leurs responsabilités en tant que telles.</p>	
<p>3.7 Assurer que les politiques de sécurité et les procédures opérationnelles pour la protection des données de titulaires de carte sont documentées, utilisées et connues de toutes les parties concernées.</p>	<p>3.7 Examiner la documentation et interroger le personnel pour vérifier que les politiques de sécurité et les procédures opérationnelles pour la protection des données de titulaires de carte stockées sont :</p> <ul style="list-style-type: none"> • Documentées, • Utilisées et • Connues de toutes les parties concernées. 	<p>Le personnel doit être conscient et suivre les politiques de sécurité et les procédures opérationnelles documentées pour la gestion du stockage sécurisé des données de titulaires de carte sur une base continue.</p>

Condition 4 : Crypter la transmission des données de titulaires de carte sur les réseaux publics ouverts

Les informations sensibles doivent être cryptées pendant leur transmission sur des réseaux accessibles à des individus malveillants. Les réseaux sans-fil mal configurés et les vulnérabilités dans les protocoles traditionnels de cryptage et d'authentification sont les cibles permanentes des individus malveillants qui profitent de ces faiblesses pour obtenir un accès privilégié aux environnements des données de titulaires de carte.

Conditions PCI DSS	Procédures de test	Directive
<p>4.1 Utiliser une cryptographie robuste et des protocoles de sécurité afin de protéger les données de titulaires de carte sensibles lors de leur transmission sur des réseaux publics ouverts, y compris :</p> <ul style="list-style-type: none"> • Seuls des clés et certificats approuvés sont acceptés. • Le protocole utilisé prend uniquement en charge les versions ou configurations sécurisées. • La force du cryptage est appropriée pour la méthodologie de cryptage employée. <p>Remarque : Les conditions dans l'annexe A2 doivent être remplies avec l'utilisation du SSL/TLS initial.</p> <p>Voici quelques exemples, parmi d'autres, de réseaux publics ouverts :</p> <ul style="list-style-type: none"> • Internet, • Technologies sans-fil, y compris 802.11 et Bluetooth • Les technologies cellulaires, par exemple, Système global pour les communications mobiles (GSM), Accès multiple de division de code (CDMA) • GPRS (service général de radiocommunication en mode paquet) • Communications par satellite 	<p>4.1.a Identifier tous les emplacements où les données de titulaires de carte sont transmises ou reçues sur des réseaux publics ouverts. Examiner les normes documentées et comparer aux configurations de système pour vérifier l'utilisation de protocoles de sécurité et l'utilisation d'une cryptographie robuste pour tous les emplacements.</p> <p>4.1.b Examiner les politiques et les procédures documentées pour vérifier que des processus sont documentés pour les points suivants :</p> <ul style="list-style-type: none"> • Pour l'acceptation exclusive des clés/certificats approuvés • Pour que le protocole utilisé prenne uniquement en charge les versions ou configurations sécurisées (pour que les versions ou configurations non sécurisées ne soient pas prises en charge) • Pour l'implémentation d'un niveau de cryptage approprié pour la méthodologie de cryptage employée <p>4.1.c Sélectionner et observer un échantillon de transmissions entrantes et sortantes à mesure qu'elles surviennent (par exemple, en observant les processus systèmes ou le trafic réseau) afin de vérifier que toutes les données de titulaires de carte sont cryptées à l'aide d'une cryptographie robuste pendant le transfert.</p> <p>4.1.d Examiner les clés et les certificats pour vérifier que seuls des clés/certificats approuvés sont acceptés.</p> <p>4.1.e Examiner les configurations de système pour vérifier que le protocole est déployé de manière à n'utiliser que des configurations sécurisées et qu'il ne prend en charge aucune version ou configuration non sécurisée.</p>	<p>Les informations sensibles doivent être cryptées durant leur transmission sur des réseaux publics, car il est facile et courant qu'un individu malveillant les intercepte et/ou les détourne pendant cette opération.</p> <p>La transmission sécurisée des données de titulaires de carte nécessite des clés/certificats fiables, un protocole sécurisé pour le transport et un cryptage d'une force suffisante pour le codage des données de titulaires de carte. Les demandes de connexion de systèmes qui ne prennent pas en charge le cryptage de la robustesse requise, et qui provoqueraient une connexion non sécurisée, ne doit pas être accepté.</p> <p>Noter que la mise en œuvre de certains protocoles (comme SSL, SSH v1.0 et TLS) a des vulnérabilités connues qu'un pirate peut utiliser pour obtenir le contrôle du système concerné. Quel que soit le protocole de sécurité utilisé, s'assurer qu'il est configuré de manière à utiliser uniquement les versions et les configurations sécurisées pour empêcher l'utilisation d'une connexion non sécurisée. Pour ce faire, utiliser uniquement des certificats autorisés et accepter uniquement un cryptage fiable (refuser les protocoles ou les méthodes affaiblis et non sécurisés).</p> <p>Vérifier que les certificats sont des certificats de confiance (par exemple, qu'ils ne sont pas arrivés à expiration et qu'ils proviennent d'une source autorisée) aide à assurer l'intégrité de la connexion sécurisée.</p>

Conditions PCI DSS	Procédures de test	Directive
	<p>4.1.f Examiner les configurations du système pour vérifier que le niveau de cryptage approprié est mis en œuvre pour la méthodologie de cryptage employée. (Vérifier les recommandations/meilleures pratiques du fournisseur.)</p>	<p><i>(suite à la page suivante)</i></p>
	<p>4.1.g Pour les mises en œuvre d'un TLS, examiner les configurations système pour vérifier que le TLS est activé lorsque les données de titulaires de carte sont transmises ou reçues.</p> <p>Par exemple, pour les implémentations basées sur le navigateur :</p> <ul style="list-style-type: none"> • La mention « HTTPS » apparaît comme protocole de l'adresse URL (Universal Record Locator, localisateur uniforme de ressource) du navigateur et • Les données de titulaires de carte sont uniquement requises lorsque la mention « HTTPS » apparaît dans l'adresse URL. 	<p>Généralement, l'URL de la page Web doit commencer par « HTTPS » et/ou une icône de cadenas apparaît dans la fenêtre du navigateur. De nombreux fournisseurs de certificats TLS apportent également un sceau de vérification haute visibilité, parfois dénommé « sceau de sécurité », « sceau de site sécurisé » ou « sceau de sécurisation de confiance », qui vous permet de cliquer sur le sceau pour afficher des informations sur le site Web.</p> <p>Consulter les normes sectorielles et les meilleures pratiques pour obtenir des informations sur une cryptographie robuste et des protocoles sécurisés (par exemple, NIST SP 800-52 et SP 800-57, OWASP, etc.)</p>
	<p>4.1.h En cas d'utilisation du SSL/TLS initial, suivez les procédures de test dans <i>l'Annexe A2 : Autres conditions de la norme PCI DSS s'appliquant aux entités qui utilisent le SSL/TLS initial.</i></p>	

Conditions PCI DSS	Procédures de test	Directive
<p>4.1.1 S'assurer que les réseaux sans fil, sur lesquels sont transmises les données de titulaires de carte ou qui sont connectés à l'environnement des données de titulaires de carte, utilisent les meilleures pratiques du secteur pour appliquer un cryptage robuste pour l'authentification et la transmission.</p>	<p>4.1.1 Identifier tous les réseaux sans-fil qui transmettent des données de titulaires de carte ou qui sont connectés à l'environnement de données de titulaires de carte. Examiner les normes documentées et comparer aux réglages de configurations de système pour vérifier les points suivants pour tous les réseaux sans-fil identifiés :</p> <ul style="list-style-type: none"> • Les meilleures pratiques du secteur sont utilisées pour l'implémentation d'un cryptage robuste à des fins d'authentification et de transmission. • Aucun cryptage faible (par exemple WEP, SSL) n'est utilisé comme contrôle de sécurité à des fins d'authentification ou de transmission. 	<p>Les utilisateurs malveillants emploient des outils gratuits et largement répandus pour écouter les communications sans-fil. L'utilisation d'une cryptographie robuste peut aider à limiter la divulgation d'informations sensibles sur les réseaux sans-fil.</p> <p>Une cryptographie robuste pour l'authentification et la transmission des données de titulaires de carte est obligatoire pour empêcher les utilisateurs malveillants d'accéder au réseau sans-fil ou d'utiliser les réseaux sans-fil pour accéder à d'autres données ou réseaux internes.</p>
<p>4.2 Ne jamais envoyer de PAN non protégés à l'aide de technologies de messagerie pour les utilisateurs finaux (par exemple e-mail, messagerie instantanée, SMS, chat, etc.).</p>	<p>4.2.a Si des technologies de messagerie d'un utilisateur final sont utilisées, observer les processus d'envoi de PAN et examiner un échantillon de transmissions sortantes lorsqu'elles ont lieu pour vérifier que le PAN est rendu illisible ou sécurisé par une cryptographie robuste chaque fois qu'il est envoyé à l'aide de technologies de messagerie d'utilisateurs finaux.</p> <p>4.2.b Examiner les politiques écrites pour vérifier l'existence d'une politique interdisant la transmission de PAN non protégés à l'aide de technologies de messagerie d'utilisateurs finaux.</p>	<p>La messagerie électronique, la messagerie instantanée, le SMS et le chat peuvent être facilement interceptés par reniflage de paquets durant l'envoi aux réseaux internes et publics. N'utiliser ces outils de messagerie pour envoyer de PAN à moins qu'ils ne soient configurés pour intégrer des fonctions de cryptage robustes.</p> <p>En outre, si une entité demande un PAN par le truchement de technologies de messagerie pour utilisateurs finaux, l'entité doit aussi fournir un outil ou une méthode pour protéger ce PAN à l'aide d'une cryptographie robuste ou rendre ce PAN illisible lors de sa transmission.</p>
<p>4.3 Assurer que les politiques de sécurité et les procédures opérationnelles pour le cryptage des données de titulaires de carte sont documentées, utilisées et connues de toutes les parties concernées.</p>	<p>4.3 Examiner la documentation et interroger le personnel pour vérifier que les politiques de sécurité et les procédures opérationnelles pour la protection des données de titulaires de carte stockées sont :</p> <ul style="list-style-type: none"> • Documentées, • Utilisées et • Connues de toutes les parties concernées. 	<p>Le personnel doit être conscient et suivre les politiques de sécurité et les procédures opérationnelles pour la gestion de la transmission sécurisée des données de titulaires de carte sur une base continue.</p>

Gestion d'un programme de gestion des vulnérabilités

Condition 5 : Protéger tous les systèmes contre les logiciels malveillants et mettre à jour régulièrement les logiciels anti-virus ou programmes

Des logiciels malicieux, généralement appelés « logiciels malveillants », par exemple virus, vers et chevaux de Troie, sont infiltrés dans le réseau dans le cadre d'activités professionnelles approuvées, notamment l'échange d'e-mails et l'accès à Internet des employés ainsi que l'utilisation de périphériques de stockage et d'ordinateurs portables. Les vulnérabilités des systèmes peuvent alors être exploitées à des fins malveillantes. Des logiciels antivirus doivent être installés sur tous les systèmes régulièrement affectés par des logiciels malveillants afin de les protéger contre les menaces logicielles actuelles et futures. Des solutions contre les logiciels malveillants supplémentaires peuvent être envisagées en complément du logiciel anti-virus ; toutefois, ces solutions supplémentaires ne supplantent pas le besoin de mise en place d'un logiciel anti-virus.

Conditions PCI DSS	Procédures de test	Directive
5.1 Déployer des logiciels antivirus sur tous les systèmes régulièrement affectés par des logiciels malveillants (en particulier PC et serveurs).	5.1 Sur un échantillon de composants de système comprenant tous les types de systèmes d'exploitation généralement affectés par des logiciels malveillants, vérifier que des logiciels antivirus sont déployés et, le cas échéant, qu'une technologie de protection antivirus est en place.	Les systèmes normalement sécurisés sont l'objet d'attaques constantes utilisant les codes d'exploitation largement publiés, souvent de type « jour zéro » (une attaque exploitant des vulnérabilités inconnues jusqu'à présent). En l'absence de solution antivirus régulièrement mise à jour, ces nouvelles formes de logiciel malveillant peuvent attaquer les systèmes et désactiver un réseau ou compromettre les données.
5.1.1 S'assurer que tous les programmes anti-virus sont capables de détecter et d'éliminer tous les types de logiciel malveillant connus, et d'assurer une protection efficace.	<p>5.1.1 Examiner la documentation du fournisseur et examiner les configurations d'anti-virus pour vérifier que les programmes d'anti-virus :</p> <ul style="list-style-type: none"> • Détectent tous les types de logiciel malveillant connus, • Éliminent tous les types de logiciel malveillant connus et • Protègent contre tous les types de logiciel malveillant connus. <p><i>Les exemples de types de logiciel malveillant connus comprennent les virus, les chevaux de Troie, les vers, les logiciels espions et publicitaires et les logiciels malveillants furtifs.</i></p>	Il est important de se protéger contre TOUS les types et formes de logiciel malveillant.

Conditions PCI DSS	Procédures de test	Directive
<p>5.1.2 Pour les systèmes considérés comme n'étant pas affectés par les logiciels malveillants, effectuer des évaluations régulières pour identifier et évaluer l'évolution de la menace posée par les logiciels malveillants afin de confirmer que ces systèmes continuent d'opérer sans logiciel anti-virus.</p>	<p>5.1.2 Interroger le personnel pour vérifier que l'évolution de la menace posée par les logiciels malveillants est surveillée et évaluée pour les systèmes n'étant pas actuellement considérés comme étant pas communément affectés par les logiciels malveillants, afin de confirmer que ces systèmes continuent d'opérer sans logiciel anti-virus.</p>	<p>Habituellement, les systèmes d'unité centrale, les ordinateurs de moyenne gamme (tels que AS/400) et les systèmes similaires ne sont pas communément ciblés ou attaqués par les logiciels malveillants. Toutefois, les tendances du secteur en matière de logiciels malveillants peuvent changer rapidement, il est donc important que les organisations soient conscientes des nouveaux logiciels malveillants qui pourraient affecter leur système, par exemple en surveillant les avis de sécurité des fournisseurs et les groupes d'information consacrés aux anti-virus pour déterminer si leur système pourrait être menacé par de nouveaux logiciels malveillants.</p> <p>Les tendances liées aux logiciels malveillants doivent être incluses dans l'identification des nouvelles vulnérabilités en matière de sécurité et les méthodes de résolution correspondantes doivent être intégrées aux normes de configuration et aux mécanismes de protection de l'entreprise, comme requis.</p>
<p>5.2 Assurer que tous les mécanismes antivirus sont maintenus comme suit :</p> <ul style="list-style-type: none"> • Maintenus à jour • Effectuent régulièrement des scans • Génèrent des journaux d'audit qui sont conservés selon la condition 10.7 de la norme PCI DSS. 	<p>5.2.a Examiner les politiques et les procédures pour vérifier que les logiciels et les définitions d'anti-virus sont conservées à jour.</p> <p>5.2.b Examiner les configurations anti-virus, y compris l'installation du logiciel maître, pour vérifier que les mécanismes anti-virus sont :</p> <ul style="list-style-type: none"> • Configurés pour effectuer automatiquement les mises à jour et • Configurées pour effectuer régulièrement des scans <p>5.2.c Examiner un échantillon de composants de système, y compris tous les types de systèmes d'exploitation généralement affectés par des logiciels malveillants, pour vérifier que :</p> <ul style="list-style-type: none"> • Le logiciel anti-virus et les définitions sont à jour. • Des scans sont effectués régulièrement. 	<p>Même les meilleures solutions anti-virus sont limitées du point de vue de l'efficacité si elles ne sont pas maintenues et mises à jour avec les dernières mises à jour de sécurité, fichiers de signature ou protection contre les logiciels malveillants.</p> <p>Les journaux d'audit permettent de surveiller l'activité des virus et des logiciels malveillants, ainsi que les réactions contre les logiciels malveillants. Par conséquent, il est impératif que la solution antivirus soit configurée pour générer des journaux d'audit et de gérer ces derniers conformément à la condition 10.</p>

Conditions PCI DSS	Procédures de test	Directive
	<p>5.2.b Examiner les configurations anti-virus, y compris l'installation du logiciel maître et un échantillon des composants de système pour vérifier que :</p> <ul style="list-style-type: none">• La production de journaux de logiciel anti-virus est activée et• Les journaux sont conservés conformément à la condition 10.7 de la norme PCI DSS.	

Conditions PCI DSS	Procédures de test	Directive
<p>5.3 Assurer que les mécanismes anti-virus fonctionnent de manière active et ne peuvent pas être désactivés ou altérés par les utilisateurs, sauf autorisation spécifique de la direction au cas par cas, sur une base limitée dans le temps.</p> <p>Remarque : <i>Les solutions anti-virus peuvent être désactivées temporairement uniquement s'il existe un besoin technique légitime, autorisé par la direction au cas par cas. Si la protection anti-virus doit être désactivée dans un but spécifique, cette désactivation doit donner lieu à une autorisation formelle. Des mesures de sécurité supplémentaires doivent également être mises en œuvre pour la période de temps pendant laquelle la protection anti-virus n'est pas active.</i></p>	<p>5.3.a Examiner les configurations anti-virus, y compris l'installation du logiciel maître et un échantillon des composants de système pour vérifier que le logiciel anti-virus fonctionne activement.</p> <p>5.3.b Examiner les configurations anti-virus, y compris l'installation du logiciel maître et un échantillon des composants de système pour vérifier que le logiciel anti-virus ne peut pas être désactivé ou altéré par les utilisateurs.</p> <p>5.3.c Interroger le personnel responsable et observer les processus pour vérifier que les logiciels anti-virus ne peuvent pas être désactivés ou altérés par les utilisateurs, sauf autorisation spécifique de la direction au cas par cas, sur une base limitée dans le temps.</p>	<p>Un anti-virus qui fonctionne continuellement et qui ne peut pas être altéré offrira une sécurité persistante contre les logiciels malveillants.</p> <p>L'utilisation de contrôles basés sur une politique sur tous les systèmes pour assurer que les protections contre les logiciels malveillants ne puissent pas être altérées ou désactivées aidera à empêcher que les faiblesses du système ne soient exploitées par les logiciels malveillants.</p> <p>Des mesures de sécurité supplémentaires peuvent également être mises en œuvre pour la période pendant laquelle la protection anti-virus n'est pas active, par exemple déconnecter le système sans protection d'Internet lorsque la protection anti-virus est désactivée, et effectuer un scan complet une fois qu'elle est réactivée.</p>
<p>5.4 Assurer que les politiques de sécurité et les procédures opérationnelles pour la protection contre les logiciels malveillants sont documentées, utilisées et connues de toutes les parties concernées.</p>	<p>5.4 Examiner la documentation et interroger le personnel pour vérifier que les politiques de sécurité et les procédures opérationnelles pour la protection contre les logiciels malveillants sont :</p> <ul style="list-style-type: none"> • Documentées • Utilisées et • Connues de toutes les parties concernées. 	<p>Le personnel doit être conscient et suivre les politiques de sécurité et les procédures opérationnelles pour garantir que les systèmes sont protégés contre les logiciels malveillants sur une base continue.</p>

Condition 6 : Développer et maintenir des systèmes et des applications sécurisés

Des individus sans scrupules peuvent exploiter les points faibles de la sécurité pour obtenir un accès privilégié aux systèmes. Bon nombre de ces vulnérabilités sont résolues par les correctifs de sécurité développés par les fournisseurs. Ceux-ci doivent être installés par les entités chargées de la gestion des systèmes. Tous les systèmes doivent être dotés des correctifs logiciels appropriés afin d'empêcher l'exploitation et l'altération des données de titulaires de carte par des individus et des logiciels malveillants.

Remarque : Les correctifs logiciels appropriés sont ceux qui ont été suffisamment évalués et testés pour déterminer qu'ils ne présentent aucun conflit avec les configurations de sécurité existantes. De nombreuses vulnérabilités peuvent être évitées dans les applications développées en interne grâce à l'utilisation de processus de développement système standard et de techniques de codage sécurisées.

Conditions PCI DSS	Procédures de test	Directive
<p>6.1 Établir un processus pour identifier les vulnérabilités de la sécurité, en utilisant des sources externes de bonne réputation pour la sécurité des informations concernant la vulnérabilité et affecter un classement du risque (par exemple « élevé », « moyen » ou « faible ») aux vulnérabilités de sécurité nouvellement découvertes.</p> <p>Remarque : Le classement des risques doit se baser sur les meilleures pratiques du secteur, ainsi que sur la prise en compte de l'impact potentiel. Par exemple, les critères de classement des vulnérabilités peuvent inclure la prise en compte du score de base CVSS et/ou la classification par le fournisseur et/ou le type de système affecté.</p> <p>Les méthodes d'évaluation de vulnérabilité et d'affectation des classements de risque varieront selon l'environnement de l'organisation et la stratégie d'évaluation des risques. Le classement de risque doit, au minimum, identifier toutes les vulnérabilités considérées comme posant un « risque élevé » pour l'environnement. En plus du classement de risque, les vulnérabilités peuvent être considérées comme « critiques » si elles constituent une menace imminente pour l'environnement, ont un impact critique sur les systèmes et/ou si elles</p>	<p>6.1.a Examiner les politiques et les procédures pour vérifier que les processus sont définis pour les points suivants :</p> <ul style="list-style-type: none"> • Pour identifier les nouvelles vulnérabilités de la sécurité • Pour assigner un classement du risque des vulnérabilités qui comprend une identification des vulnérabilités à « haut risque » et des vulnérabilités « critiques ». • Pour utiliser des sources externes fiables pour les informations sur les vulnérabilités en matière de sécurité <p>6.1.b Interroger le personnel responsable et examiner le processus pour vérifier que :</p> <ul style="list-style-type: none"> • Les nouvelles vulnérabilités de la sécurité sont identifiées. • Une classification des risques est affectée aux vulnérabilités. Elle comprend une identification de toutes les vulnérabilités à « haut risque » et « critiques ». • Des processus pour identifier les nouvelles vulnérabilités de sécurité comprennent l'utilisation des sources externes d'information sur la vulnérabilité de sécurité. 	<p>L'objectif de cette condition est de faire en sorte que les organisations restent à jour et informées des nouvelles vulnérabilités pouvant affecter leur environnement.</p> <p>Les sources d'informations concernant la vulnérabilité doivent être fiables et elles comprennent souvent les sites Web des fournisseurs, les groupes d'information du secteur, les listes de diffusion ou flux RSS.</p> <p>Une fois qu'une organisation identifie une vulnérabilité qui pourrait affecter son environnement, le risque posé par cette vulnérabilité doit être évalué et classé. L'organisation doit donc avoir mis en place une méthode pour évaluer les vulnérabilités sur une base continue et affecter un classement du risque posé par ces vulnérabilités. Cet objectif n'est pas atteint avec un scan ASV ou un scan de vulnérabilité interne, un processus est nécessaire pour surveiller de manière active les sources de l'industrie pour connaître les informations portant sur les vulnérabilités.</p> <p>Établir un classement des risques (par exemple, « élevé », « moyen » et « faible ») permet aux organisations d'identifier et de répondre plus rapidement aux éléments de risque de priorité élevée, et de réduire la probabilité que les vulnérabilités impliquant les risques les plus élevés soient exploitées.</p>

Conditions PCI DSS	Procédures de test	Directive
<p>sont susceptibles de compromettre l'application si elles ne sont pas résolues. Les exemples de systèmes critiques peuvent inclure les systèmes de sécurité, les dispositifs et systèmes ouverts au public, les bases de données et autres systèmes qui stockent, traitent ou transmettent des données de titulaires de carte.</p>		
<p>6.2 S'assurer que tous les logiciels et les composants de système sont protégés de vulnérabilité connues en installant les correctifs de sécurité applicables fournis par le fournisseur. Installer les correctifs de sécurité stratégiques dans le mois qui suit leur commercialisation.</p> <p>Remarque : Les correctifs de sécurité critiques doivent être identifiés selon le processus de classement des risques défini par la condition 6.1.</p>	<p>6.2.a Examiner les politiques et les procédures les politiques relatives à l'installation des correctifs de sécurité pour vérifier que les processus sont définis pour :</p> <ul style="list-style-type: none"> • Installer les correctifs de sécurité critiques pertinents fournis par le fournisseur dans le mois qui suit leur commercialisation. • Installer tous les correctifs de sécurité critiques pertinents fournis par le fournisseur dans un délai acceptable (par exemple, dans les trois mois). <p>6.2.b Pour un échantillon de composants de système et de logiciels associés, comparer la liste des correctifs de sécurité installés sur chaque système avec la liste des correctifs de sécurité les plus récents du fournisseur, pour vérifier les points suivants :</p> <ul style="list-style-type: none"> • Les correctifs de sécurité critiques pertinents fournis par le fournisseur sont installés dans le mois qui suit leur commercialisation. • Tous les correctifs pertinents de sécurité fournis par le fournisseur sont installés dans un délai acceptable (par exemple, dans les trois mois). 	<p>Les systèmes normalement sécurisés sont l'objet d'attaques constantes utilisant les codes d'exploitation largement publiés, souvent de type « jour zéro » (une attaque exploitant des vulnérabilités inconnues jusqu'à présent). Si les correctifs les plus récents ne sont pas mis en œuvre dès que possible sur les systèmes critiques, un individu malveillant pourrait exploiter cette faiblesse pour attaquer ou désactiver un système ou pour accéder à des données sensibles.</p> <p>Établir une priorité des correctifs pour l'infrastructure critique garantit que les systèmes et les dispositifs de haute priorité sont protégés des vulnérabilités aussi tôt que possible après la commercialisation d'un correctif. Envisager donner la priorité à l'installation de correctif, de sorte que les correctifs de sécurité pour les systèmes critiques ou à risque soient installés dans les 30 jours et les correctifs de sécurité moins critique dans les 2-3 mois.</p> <p>Cette condition s'applique à tous les correctifs applicables pour tous les logiciels installés, y compris les applications de paiement (celles qui sont validées et non validées par PA-DSS).</p>
<p>6.3 Développer des applications logicielles internes et externes (y compris l'accès administratif aux applications par le Web) conformément aux points suivants :</p> <ul style="list-style-type: none"> • Conformément à la norme PCI DSS (par exemple, authentification et connexion sécurisées) 	<p>6.3.a Examiner les processus écrits de développement de logiciel pour vérifier qu'ils se basent sur les normes du secteur et/ou les meilleures pratiques.</p> <p>6.3.b Examiner les processus écrits de développement de logiciel pour vérifier que la sécurité des informations est intégrée à tout le cycle de vie.</p>	<p>Faute d'intégrer la sécurité aux phases de définition des conditions, de conception, d'analyse et de test du développement d'un logiciel, des vulnérabilités de sécurité peuvent être introduites, accidentellement ou par malveillance, dans l'environnement de production.</p>

Conditions PCI DSS	Procédures de test	Directive
<ul style="list-style-type: none"> Basés sur les normes/meilleures pratiques du secteur. Incorporer la sécurité des informations de sécurité au cours du cycle de vie de la conception d'un logiciel. <p><i>Note : ce point s'applique à tous les logiciels développés à l'interne, ainsi qu'aux logiciels sur mesure ou personnalisés qui sont développés par un tiers.</i></p>	<p>6.3.c Examiner les processus écrits de développement de logiciel pour vérifier que les applications logicielles sont développées conformément à la norme PCI DSS.</p> <p>6.3.d Interroger les développeurs de logiciel pour vérifier que les processus écrits de développement de logiciel sont mis en œuvre.</p>	<p>Comprendre comment les données sensibles sont traitées par l'application, y compris lorsqu'elles sont stockées, transmises et lorsqu'elles sont en mémoire peut aider à identifier l'emplacement où les données ont besoin d'être protégées.</p>
<p>6.3.1 Supprimer les comptes de développement, de test et/ou les comptes d'application personnalisés, les ID d'utilisateur et des mots de passe avant l'activation des applications ou leur mise à la disposition des clients.</p>	<p>6.3.1 Examiner les procédures écrites de développement de logiciel et interroger le personnel responsable pour vérifier que les comptes de pré-production et/ou les comptes d'application personnalisée, les ID d'utilisateur et/ou les mots de passe sont éliminés avant qu'une application entre en production ou sont mise à disposition des clients.</p>	<p>Les comptes d'application personnalisés et/ou de test, les ID utilisateur et les mots de passe doivent être supprimés du code de production avant l'activation de l'application ou sa mise à la disposition des clients puisque ces éléments peuvent révéler des informations sur le fonctionnement de l'application. Grâce à la possession de ces informations, il est plus facile de compromettre l'application et les données de titulaires de carte associées.</p>

Conditions PCI DSS	Procédures de test	Directive
<p>6.3.2 Examiner le code d'application personnalisé avant la mise en production ou la mise à la disposition des clients afin d'identifier toute vulnérabilité de codage éventuelle (à l'aide de processus manuels ou automatiques) pour inclure au moins les points suivants :</p> <ul style="list-style-type: none"> • Les modifications de code sont examinées par des individus autres que l'auteur initial du code et par des individus compétents en la matière de techniques d'analyse de code et de pratiques de codage sécurisées. • Les examens de code garantissent que le code est développé conformément aux bonnes pratiques de codage sécurisé • Les corrections appropriées sont implémentées avant la publication. • Les résultats de l'examen du code sont passés en revue et approuvés par les responsables avant le lancement. <p style="text-align: right;"><i>(suite à la page suivante)</i></p>	<p>6.3.2.a Examiner les procédures écrites de développement de logiciel et interroger le personnel responsable pour tous les changements d'applications personnalisées doivent être analysés (à l'aide de processus manuels ou automatiques) comme suit :</p> <ul style="list-style-type: none"> • Les modifications de code sont examinées par des individus autres que l'auteur initial du code, qui doivent être compétents en la matière et maîtriser les pratiques de codage sécurisées. • Les examens du code garantissent que le code est développé conformément aux bonnes pratiques de codage sécurisé (voir la condition 6.5 de la norme PCI DSS). • Les corrections appropriées sont implémentées avant la publication. • Les résultats de l'examen du code sont passés en revue et approuvés par les responsables avant le lancement. 	<p>Les vulnérabilités de sécurité du code personnalisé sont généralement exploitées par les individus malveillants pour accéder à un réseau et compromettre les données de titulaires de carte.</p> <p>Une personne compétente et expérimentée en matière de techniques d'analyse de code doit prendre part au processus d'analyse. Les analyses de code doivent être effectuées par une personne autre que le développeur du code, afin que le contrôle puisse être indépendant et objectif. Des outils ou processus automatiques peuvent également être utilisés alternativement aux analyses manuelles, mais soyez conscient du fait qu'il pourrait être difficile ou même impossible pour un outil automatique d'identifier certains problèmes de codage.</p> <p>La correction des erreurs de codage avant que le code ne soit déployé dans un environnement de production ou mis à la disposition des clients empêche que le code n'expose l'environnement aux exploitations indésirables. Un code défaillant est bien plus difficile et cher à résoudre après qu'il ait été déployé ou lancé dans l'environnement de production.</p> <p>Inclure un examen formel et une signature des responsables avant le lancement aide à garantir que ce code est approuvé et a été développé selon les politiques et procédures.</p>

Conditions PCI DSS	Procédures de test	Directive
<p>Remarque : Cette condition s'applique à l'intégralité du code personnalisé (aussi bien interne qu'orienté public), dans le cadre du cycle de conception du système.</p> <p>Les examens du code peuvent être réalisés par le personnel interne compétent ou par des prestataires tiers. Les applications Web destinées au public font également l'objet de contrôles supplémentaires afin de résoudre les menaces et les vulnérabilités éventuelles après leur déploiement, comme défini par la condition 6.6 de la norme PCI DSS.</p>	<p>6.3.2.b Sélectionner un échantillon de modifications apportées récemment à une application personnalisée et vérifier que le code correspondant est examiné conformément aux instructions décrites au point 6.3.2.a ci-dessus.</p>	
<p>6.4 Suivre les processus et procédures de contrôle des changements pour toutes les modifications apportées à des composants de système. Ces processus doivent inclure les points suivants :</p>	<p>6.4 Examiner les politiques et les procédures pour vérifier que les points suivants sont définis :</p> <ul style="list-style-type: none"> • Les environnements de test/développement sont distincts de l'environnement de production et il existe un contrôle d'accès pour garantir la séparation. • Il existe une séparation des tâches entre le personnel affecté aux environnements de développement/test et le personnel affecté à l'environnement de production. • Les données de production (PAN actifs) ne sont pas utilisées à fins de test ou de développement. • Les comptes et les données de test sont supprimés avant que le système de production ne devienne actif. • Les changements de procédure de contrôle relatifs à la mise en œuvre de correctifs de sécurité et aux modifications de logiciel sont documentés. 	<p>Sans un contrôle correctement documenté et implémenté des modifications, les fonctions de sécurité peuvent être accidentellement ou délibérément omises ou rendues inopérantes, des irrégularités de traitement peuvent se produire ou un code malveillant peut être introduit.</p>
<p>6.4.1 Séparer les environnements de test/développement des environnements de production et appliquer la séparation à l'aide de contrôles d'accès</p>	<p>6.4.1.a Examiner la documentation de réseau et les configurations de dispositif de réseau pour vérifier que les environnements de test/développement sont distincts de l'environnement de production.</p> <p>6.4.1.b Examiner les réglages de contrôle d'accès pour vérifier que les contrôles d'accès sont en place pour appliquer la séparation entre les environnements de test/développement et l'environnement de production.</p>	<p>En raison de leur évolution constante, les environnements de développement et de test tendent à être moins sécurisés que les environnements de production. Sans une séparation appropriée des environnements, l'environnement de production et les données de titulaires de carte pourraient être compromis en raison de configurations de sécurité moins strictes et de possibles vulnérabilités dans un environnement de test ou de développement.</p>

Conditions PCI DSS	Procédures de test	Directive
<p>6.4.2 Séparation des obligations entre les environnements de développement/test et de production.</p>	<p>6.4.2 Examiner les processus et interroger le personnel affecté aux environnements de développement/test et le personnel affecté aux environnements de production pour vérifier que la séparation des tâches est en place entre les environnements de test/développement et l'environnement de production.</p>	<p>Réduire le nombre de personnes ayant accès à l'environnement de production et aux données de titulaires de carte minimise le risque et permet de garantir que l'accès est limité aux seuls individus ayant un besoin professionnel d'en connaître.</p> <p>Cette condition est destinée à garantir la séparation entre les fonctions de test et de développement et les fonctions de production. Par exemple, un développeur peut utiliser un compte de niveau administrateur avec des privilèges de haut rang dans l'environnement de développement et posséder un compte distinct avec un accès de niveau utilisateur à l'environnement de production.</p>
<p>6.4.3 Les données de production (PAN actifs) ne sont pas utilisées à des fins de test ou de développement.</p>	<p>6.4.3.a Examiner les processus de test et interroger le personnel pour vérifier que des procédures sont en place pour garantir que les données de production (PAN actifs) ne sont plus utilisées pour le test ou le développement.</p> <p>6.4.3.b Examiner un échantillon de données de test pour vérifier que les données de production (PAN actifs) ne sont pas utilisées à fin de test ou de développement.</p>	<p>Les contrôles de sécurité ne sont généralement pas aussi stricts dans les environnements de test ou de développement. L'utilisation des données de production donne aux individus malveillants la possibilité d'y accéder (données de titulaires de carte) sans y être autorisés.</p>
<p>6.4.4 Suppression des données et comptes de tests dans les composants de système avant que le système ne devienne actif/passe en phase de production.</p>	<p>6.4.4.a Examiner les processus de test et interroger le personnel pour vérifier que les données et les comptes de test sont éliminés avant qu'un système de production ne devienne actif.</p> <p>6.4.4.b Examiner un échantillon des données et de comptes des systèmes de production récemment installés ou mis à jour pour vérifier que les données et les comptes de test sont éliminés avant que le système de devienne actif.</p>	<p>Les données et les comptes de test doivent être supprimés avant l'activation (la production) du composant de système puisque ces éléments peuvent divulguer des informations sur le fonctionnement de l'application ou du système. Avec ces informations, il est plus facile de compromettre le système et les données de titulaires de carte associées.</p>

Conditions PCI DSS	Procédures de test	Directive
<p>6.4.5 Les procédures de contrôle de changement doivent inclure ce qui suit :</p>	<p>6.4.5.a Examiner les procédures documentées de contrôle de changement et vérifier qu'elles sont définies pour :</p> <ul style="list-style-type: none"> • Documentation de l'impact • Approbation de changement documentée par les parties autorisées • Test de fonctionnalité pour vérifier que le changement ne compromet pas la sécurité du système. • Procédures de suppression <p>6.4.5.b Pour un échantillon de composants de système, interroger le personnel responsable pour déterminer les changements récents. Retracer ces changements sur la documentation de contrôle des changements associés. Pour chaque modification étudiée, procéder comme suit :</p>	<p>En cas de gestion inadéquate, l'impact des changements du système (comme les mises à jour matérielles ou logicielles et l'installation de correctifs de sécurité) peut ne pas être pleinement effectif et pourrait avoir des conséquences non intentionnelles.</p>
<p>6.4.5.1 Documentation de l'impact.</p>	<p>6.4.5.1 Vérifier que la documentation de l'impact est comprise dans la documentation de contrôle des changements, et ce pour chaque changement inclus dans l'échantillon.</p>	<p>L'impact de la modification doit être documenté de sorte que toutes les parties concernées soient en mesure de planifier en conséquence pour tout changement du traitement.</p>
<p>6.4.5.2 Documentation du changement approuvée par les parties autorisées.</p>	<p>6.4.5.2 Vérifier qu'une approbation documentée par les responsables existe pour chaque modification échantillonnée.</p>	<p>L'approbation par les responsables autorisés indique que la modification est légitime et que son approbation est ratifiée par l'organisation.</p>
<p>6.4.5.3 Test de fonctionnalité pour vérifier que le changement ne compromet pas la sécurité du système.</p>	<p>6.4.5.3.a Pour chaque changement échantillonné, vérifier que le test de fonctionnalité a été exécuté pour vérifier que le changement ne compromet pas la sécurité du système.</p> <p>6.4.5.3.b Pour les modifications de code personnalisé, vérifier la conformité à la condition 6.5 de la norme PCI DSS de toutes les mises à jour avant leur mise en production.</p>	<p>Un test approfondi doit être effectué afin de vérifier que la sécurité de l'environnement n'est pas diminuée par la mise en œuvre d'une modification. Le test doit valider que tous les contrôles de sécurité existants restent en place, sont remplacés par des contrôles de force équivalente, ou sont renforcés après toute modification de l'environnement.</p>
<p>6.4.5.4 Procédures de suppression.</p>	<p>6.4.5.4 Vérifier que des procédures de suppression sont préparées pour chaque changement inclus dans l'échantillon.</p>	<p>Pour chaque modification, il doit exister des procédures de retrait documentées au cas où la modification échouerait ou aurait des effets néfastes sur la sécurité de l'application ou du système, afin de pouvoir restaurer le système à son état antérieur.</p>

Conditions PCI DSS	Procédures de test	Directive
<p>6.4.6 Suite à un changement important, toutes les conditions pertinentes PCI DSS doivent être mises en œuvre sur tous les systèmes et réseaux, qu'ils soient nouveaux ou modifiés, et la documentation est mise à jour, le cas échéant.</p> <p><i>Remarque : Cette condition est considérée comme une meilleure pratique jusqu'au 31 janvier 2018, après quoi ce sera une obligation.</i></p>	<p>6.4.6 Pour un échantillon de changements importants, examiner les registres de changements, interroger le personnel et observer les systèmes/réseaux concernés pour s'assurer que les conditions applicables de la norme PCI DSS ont été effectivement implémentées et que la documentation a bien été mise à jour dans le cadre de ces changements.</p>	<p>L'existence de processus destinés à l'analyse de changements importants permet de s'assurer que tous les contrôles appropriés de la norme PCI DSS sont effectivement appliqués aux systèmes/réseaux ajoutés ou modifiés dans l'environnement concerné.</p> <p>L'insertion de cette validation dans les processus de gestion des changements vous permet de garantir que les inventaires de dispositifs et les normes de configuration sont mis à jour et que les contrôles de sécurité sont appliqués en fonction des besoins.</p> <p>Un processus de gestion des changements doit contenir des éléments justificatifs pour illustrer la mise en œuvre ou la conservation des conditions de la norme PCI DSS par le biais d'un processus itératif. Voici des exemples, sans s'y limiter, des conditions PCI DSS susceptibles d'être concernées :</p> <ul style="list-style-type: none"> • Le schéma du réseau est mis à jour pour illustrer les changements. • Les systèmes sont configurés conformément aux normes de configuration ; tous les mots de passe par défaut sont modifiés et les services superflus sont désactivés. • Les systèmes sont protégés par des contrôles obligatoires, comme le contrôle de l'intégrité des fichiers (file-integrity monitoring, FIM), le programme antivirus, les correctifs et la journalisation d'audit. • Les données d'identification sensibles (SAD) ne sont pas stockées et le stockage de toutes les données de titulaires de carte est documenté et incorporé à la politique et aux procédures relatives à la conservation de données. • Les nouveaux systèmes sont inclus dans le processus d'analyse trimestrielle des vulnérabilités.

Conditions PCI DSS	Procédures de test	Directive
<p>6.5 Adresser les vulnérabilités de code les plus fréquentes dans les processus de développement de logiciel, afin d'inclure les éléments suivants :</p> <ul style="list-style-type: none"> • Former les développeurs au moins une fois par an pour perfectionner leurs techniques de codage sécurisé, afin qu'ils sachent notamment comment éviter les vulnérabilités de codage courantes. • Développer des applications basées sur les directives de codage sécurisé. <p>Remarque : Les vulnérabilités décrites aux points 6.5.1 à 6.5.10 faisaient partie des meilleures pratiques du secteur au moment de la publication de cette version de la norme PCI DSS. Cependant, comme les meilleures pratiques de gestion de la vulnérabilité du secteur sont actualisées (par exemple, le guide OWASP, le Top 25 SANS CWE, le codage sécurisé CERT, etc.), se reporter aux meilleures pratiques actuelles pour ces conditions.</p>	<p>6.5.a Examiner les politiques et les procédures de développement logiciel pour vérifier que la formation aux techniques de codage sécurisé est requise pour les développeurs au moins une fois par an et en fonction des meilleures pratiques et directives de l'industrie.</p> <p>6.5.b Examiner les registres de formation pour vérifier que les développeurs logiciels ont été formés aux dernières techniques de codage sécurisé au moins une fois par an, afin qu'ils sachent notamment comment éviter les vulnérabilités de codage courantes.</p> <p>6.5.c Vérifier la mise en place de processus pour protéger les applications, au minimum, des vulnérabilités suivantes :</p>	<p>La couche application comporte un risque élevé et peut être la cible de menaces internes et externes.</p> <p>Les conditions 6.5.1 à 6.5.10 représentent les contrôles minimums qui doivent être en place et les organisations doivent incorporer les pratiques de codage sécurisées pertinentes qui sont applicables à la technologie spécifique de leur environnement.</p> <p>Les développeurs d'application doivent être correctement formés pour identifier et résoudre les problèmes liés à ces vulnérabilités de codage courantes (et aux autres). Assurer que le personnel est compétent en matière de pratiques de codage sécurisées aidera à minimiser le nombre de vulnérabilités de la sécurité introduites par de mauvaises pratiques de codage. La formation des développeurs peut être effectuée à l'interne ou par des tiers et elle doit s'appliquer à la technologie utilisée.</p> <p>Lorsque les pratiques de codage sécurisé, acceptées par le secteur, changent, les pratiques de codage de l'organisation doivent elles aussi être mises à jour, de même que la formation des développeurs afin de répondre aux nouvelles menaces, par exemple les attaques de déchirement de mémoire.</p> <p>Les vulnérabilités identifiées de 6.5.1 à 6.5.10 représentent la ligne de base minimale. C'est à l'organisation de demeurer à jour vis-à-vis des tendances en matière de vulnérabilité et d'incorporer des mesures appropriées dans leurs pratiques de codage sécurisées.</p>

Conditions PCI DSS	Procédures de test	Directive
<p>Remarque : Les conditions 6.5.1 à 6.5.6, ci-dessous, s'appliquent à toutes les applications (internes ou externes).</p>		
<p>6.5.1 Attaques par injection, notamment les injections de commandes SQL Envisager également les attaques par injection OS, LDAP et Xpath ainsi que les autres attaques par injection.</p>	<p>6.5.1 Examiner les politiques et les procédures de développement de logiciel et interroger le personnel responsable pour vérifier que les attaques par injection sont adressées par des techniques de codage qui comprennent :</p> <ul style="list-style-type: none"> • La validation d'entrée pour vérifier que les données utilisateurs ne peuvent pas modifier le sens des commandes et des requêtes. • Utiliser des requêtes paramétrées. 	<p>Les attaques par injection, en particulier injection de commandes SQL, sont une méthode couramment utilisée pour compromettre des applications. Une attaque par injection se produit lorsque les données saisies par un utilisateur sont transmises à un programme d'interprétation dans le cadre d'une commande ou d'une requête. Les données hostiles du pirate trompent le programme d'interprétation pour lui faire exécuter des commandes non prévues ou modifier les données, permettant au pirate d'attaquer les composants du réseau par le biais de l'application, de lancer des attaques comme la saturation de la mémoire tampon, ou de révéler des informations confidentielles ainsi que la fonctionnalité de l'application serveur.</p> <p>Les informations doivent être validées avant d'être transmises à l'application, par exemple en vérifiant tous les caractères alphabétiques, le mélange de caractères alphanumériques, etc.</p>
<p>6.5.2 Saturation de la mémoire tampon</p>	<p>6.5.2 Examiner les politiques et les procédures de développement de logiciel et interroger le personnel responsable pour vérifier que les saturations de la mémoire tampon sont adressées par des techniques de codage qui comprennent :</p> <ul style="list-style-type: none"> • Validation de limites de la mémoire tampon ; • Troncage des chaînes d'entrées. 	<p>La saturation de la mémoire tampon se produit lorsqu'une application ne dispose pas de contrôles de limites sur l'espace de sa mémoire tampon. Ceci a pour résultat de pousser les informations de la mémoire tampon en dehors de son espace et dans l'espace exécutable de la mémoire. Lorsque cela se produit, le pirate a la possibilité d'insérer un code malveillant à une extrémité de la mémoire puis de le pousser dans l'espace exécutable de la mémoire en saturant la mémoire tampon. Le code malveillant est ensuite exécuté et permet souvent l'accès à distance du pirate, à l'application et/ou au système infecté.</p>

Conditions PCI DSS	Procédures de test	Directive
<p>6.5.3 Stockage cryptographique non sécurisé</p>	<p>6.5.3 Examiner les politiques et les procédures de développement de logiciel et interroger le personnel responsable pour vérifier que le stockage cryptographique non sécurisé est adressé par des techniques de codage qui comprennent :</p> <ul style="list-style-type: none"> • Il faut prévenir les défauts cryptographiques. • Utilisez des algorithmes et des clés cryptographiques robustes. 	<p>Les applications qui n'utilisent pas de robustes fonctions cryptographiques correctement pour stocker des données, présentent un risque accru d'être compromises et d'exposer les justificatifs d'authentification et/ou les données de titulaires de carte. Si un pirate est en mesure d'exploiter une faiblesse des processus cryptographiques, il peut accéder au texte clair des données cryptées.</p>
<p>6.5.4 Communications non sécurisées</p>	<p>6.5.4 Examiner les politiques et les procédures de développement de logiciel et interroger le personnel responsable pour vérifier que les communications non sécurisées sont adressées par des techniques de codage qui authentifient et cryptent correctement toutes les communications sensibles.</p>	<p>Les applications qui ne réussissent pas à correctement crypter le trafic réseau à l'aide d'une cryptographie robuste présentent un risque accru d'être compromises et d'exposer les données de titulaires de carte. Si un pirate est en mesure d'exploiter une faiblesse des processus cryptographiques, il peut se retrouver en mesure de prendre le contrôle de l'application ou même d'accéder au texte clair des données cryptées.</p>
<p>6.5.5 Traitement inapproprié des erreurs</p>	<p>6.5.5 Examiner les politiques et les procédures de développement logiciel et interroger le personnel responsable pour vérifier que le traitement inapproprié des erreurs est résolu à l'aide de techniques de codage qui ne laissent fuir aucune information par le biais de messages d'erreur (par exemple, en retournant des détails d'erreur spécifiques plutôt que génériques).</p>	<p>Les applications peuvent laisser filtrer accidentellement des informations sur leur configuration ou mécanismes internes, ou exposer des informations privilégiées en raison de méthodes de traitement incorrectes. Les pirates peuvent utiliser cette faiblesse pour subtiliser des données sensibles ou pour compromettre le système dans sa globalité. Si un individu malveillant peut créer des erreurs que l'application ne gère pas correctement, il peut alors obtenir des informations système détaillées, créer des interruptions par déni de service, mettre la sécurité en échec ou entraîner une panne de serveur. Par exemple, le message selon lequel le « mot de passe saisi est incorrect » indique à un pirate que l'ID utilisateur fourni est correct et qu'il lui suffit de concentrer ses efforts sur le décryptage du mot de passe. Utiliser des messages d'erreur plus génériques, comme « Impossible de vérifier les données ».</p>

Conditions PCI DSS	Procédures de test	Directive
<p>6.5.6 Toutes les vulnérabilités à « haut risque », identifiées dans le processus d'identification de vulnérabilité (selon la condition 6.1 de la norme PCI DSS).</p>	<p>6.5.6 Examiner les politiques et les procédures de développement de logiciel et interroger le personnel responsable pour vérifier que les techniques répondent aux vulnérabilités à « risque élevé » qui pourraient affecter l'application, comme elles sont identifiées par la condition 6.1. de la norme PCI DSS.</p>	<p>Toutes les vulnérabilités déterminées par le processus de classement des risques de vulnérabilité d'une organisation (défini dans la condition 6.1) comme étant un « risque élevé » et qui pourrait affecter l'application doivent être identifiées et résolues pendant le développement de l'application.</p>
<p>Remarque : Les conditions 6.5.7 à 6.5.10, ci-dessous, s'appliquent aux applications Web et aux interfaces d'application (internes ou externes) :</p>		<p>Les applications Web, internes et externes (publiques), comportent des risques de sécurité uniques dus à leur architecture, à leur manque de difficulté relatif et aux possibilités de les compromettre.</p>
<p>6.5.7 Script inter-site (XSS)</p>	<p>6.5.7 Examiner les politiques et les procédures de développement de logiciel et interroger le personnel responsable pour vérifier que de script inter-site (XSS) est adressé par des techniques de codage qui comprennent :</p> <ul style="list-style-type: none"> • La validation de tous les paramètres avant l'inclusion • L'utilisation d'un mécanisme d'échappement sensible au contexte. 	<p>Les attaques XSS se produisent chaque fois qu'une application extrait les données fournies par un utilisateur et les transmet à un navigateur Web sans d'abord les valider ou coder le contenu. Une attaque XSS permet aux pirates d'exécuter, dans le navigateur de la victime, un script qui peut détourner des sessions utilisateurs, rendre des sites Web illisibles, introduire éventuellement des vers, etc.</p>

Conditions PCI DSS	Procédures de test	Directive
<p>6.5.8 Contrôle d'accès inapproprié (comme des références d'objet directes non sécurisées, impossibilité de limiter l'accès URL, le survol de répertoire et la non-restriction de l'accès utilisateur aux fonctions).</p>	<p>6.5.8 Examiner les politiques et les procédures de développement de logiciel et interroger la personne responsable pour vérifier que le contrôle d'accès inapproprié, comme des références d'objet directes non sécurisées, l'impossibilité de limiter l'accès URL et le survol de répertoire, est résolu à l'aide de techniques de codage qui comprennent :</p> <ul style="list-style-type: none"> • L'authentification correcte des utilisateurs ; • L'assainissement des entrées ; • Ne pas exposer les références d'objets internes aux utilisateurs ; • Les interfaces utilisateurs qui ne permettent pas d'accéder aux fonctions non autorisées. 	<p>Une référence d'objet directe existe lorsqu'un développeur expose la référence à un objet d'implémentation interne, par exemple un fichier, un répertoire, un enregistrement de base de données ou une clé, comme une adresse URL ou un paramètre de formulaire. Les pirates peuvent manipuler ces références pour accéder à d'autres objets sans autorisation.</p> <p>Appliquer uniformément le contrôle d'accès au niveau de la couche présentation et des modèles de traitement pour toutes les URL. Fréquemment, le seul moyen qu'une application protège la fonctionnalité sensible est d'empêcher l'affichage des liens ou des URL aux utilisateurs non autorisés. Les pirates peuvent exploiter cette faiblesse pour accéder à des opérations non autorisées et les exécuter en accédant directement à ces URL.</p> <p>Un pirate peut être en mesure de détailler la structure du répertoire d'un site Web et de le parcourir (survol de répertoire), obtenant ainsi accès à des informations non autorisées ainsi que la compréhension du fonctionnement du site qu'il exploitera plus tard.</p> <p>Si les interfaces utilisateurs donnent accès à des fonctions non autorisées, cet accès pourrait permettre à des individus non autorisés d'accéder à des justificatifs privilégiés ou à des données de titulaires de carte. Seuls les utilisateurs autorisés doivent pouvoir accéder directement aux références d'objet de ressources sensibles. Limiter l'accès aux ressources de données aidera à empêcher que les données de titulaires de carte ne soient présentées à des ressources non autorisées.</p>

Conditions PCI DSS	Procédures de test	Directive
<p>6.5.9 Attaques CSRF (Cross-site request forgery)</p>	<p>6.5.9 Examiner les politiques et les procédures de développement de logiciel et interroger le personnel responsable pour vérifier que les attaques de falsification de requête inter-site (CSRF) sont résolues en utilisant des techniques de codage qui assurent que les applications ne comptent pas sur des justificatifs d'autorisation et sur des jetons soumis automatiquement par les navigateurs.</p>	<p>Une attaque CSRF force le navigateur d'une victime connectée à envoyer une requête pré-authentifiée à une application Web vulnérable, qui permet ensuite au pirate d'effectuer les opérations de changement d'état que la victime est autorisée à effectuer (comme de mettre à jour les détails de compte, effectuer des achats ou même s'authentifier envers l'application).</p>
<p>6.5.10 Rupture dans la gestion des authentifications et des sessions</p>	<p>6.5.10 Examiner les politiques et les procédures de développement de logiciel et interroger le personnel responsable pour vérifier que la rupture de la gestion des authentifications et des sessions est adressée par des techniques de codage qui comprennent :</p> <ul style="list-style-type: none"> • Étiqueter les jetons de session (par exemple les cookies) comme étant « sécurisés » • Ne pas exposer les ID de session dans l'URL • Incorporer des durées limites de session et des rotations d'ID de session avec une connexion réussie. 	<p>Sécuriser l'authentification et la gestion de session empêche les individus non autorisés de compromettre les justificatifs de compte légitimes, les clés ou les jetons de session qui, autrement, permettrait à l'intrus d'assurer l'identité d'un utilisateur autorisé.</p>

Conditions PCI DSS	Procédures de test	Directive
<p>6.6 Pour les applications Web destinées au public, traiter les nouvelles menaces et vulnérabilités de manière continue et veiller à ce que ces applications soient protégées contre les attaques connues à l'aide de l'une des méthodes suivantes :</p> <ul style="list-style-type: none"> Examen des applications Web destinées au public à l'aide d'outils ou de méthodes d'évaluation de la sécurité et de la vulnérabilité des applications automatiques ou manuelles, au moins une fois par an et après toute modification. <p>Remarque : Cette évaluation est différente des scans de vulnérabilité effectués pour la condition 11.2.</p> <ul style="list-style-type: none"> Installer une solution technique automatisée qui détecte et empêche les attaques basées sur Internet (par exemple le pare-feu d'une application Web) devant les applications web destinées au public pour vérifier continuellement tout le trafic. 	<p>6.6 Pour des applications Web destinées au public, s'assurer que l'une ou l'autre des méthodes ci-dessous est en place comme suit :</p> <ul style="list-style-type: none"> Examiner les processus documentés, interroger le personnel et examiner les archives des évaluations de sécurité de l'application pour vérifier que les applications Web destinées au public sont examinées, à l'aide d'outils ou de méthodes d'évaluation de la sécurité et de la vulnérabilité automatiques ou manuels, de la manière suivante : <ul style="list-style-type: none"> Au moins une fois par an ; Après toute modification ; Par une société spécialisée dans la sécurité des applications ; Que, au minimum, toutes les vulnérabilités de la condition 6.5 sont incluses dans l'évaluation ; Toutes les vulnérabilités sont corrigées ; Que l'application est réévaluée après les corrections. Examiner les réglages de configuration du système et interroger le personnel responsable pour vérifier qu'une solution technique automatisée qui détecte et empêche les attaques basées sur Internet (par exemple le pare-feu d'une application Web) est en place comme suit : <ul style="list-style-type: none"> Est située devant les applications Web destinées au public pour détecter et empêcher les attaques basées sur le Web. Fonctionne activement et est mise à jour au besoin. Génère des journaux d'audit. Est configurée soit pour bloquer les attaques basées sur le Web soit pour générer une alerte qui fera directement l'objet d'une enquête. 	<p>Les applications Web destinées au public sont les cibles principales des pirates et les applications Web à codage médiocre donnent un chemin d'accès facile pour les pirates qui cherchent à accéder aux données et aux systèmes sensibles. La condition de vérification des applications ou d'installation de pare-feu pour les applications Web est destinée à réduire le nombre d'attaques des applications Web destinées au public causées par un codage médiocre ou par des pratiques de gestion d'application médiocres.</p> <ul style="list-style-type: none"> Des outils ou des méthodes manuels ou automatiques d'évaluation de la sécurité et de la vulnérabilité, examinent et/ou testent les vulnérabilités de l'application Les pare-feu pour applications Web filtrent et bloquent le trafic non essentiel au niveau de la couche application. Utilisé conjointement à un pare-feu réseau, un pare-feu pour application Web correctement configuré empêche les attaques de la couche application si les applications sont mal codées ou mal configurées. Cela peut être réalisé en associant la technologie et les processus. Les solutions basées sur des processus doivent comporter des mécanismes qui facilitent des réponses rapides face aux alertes afin d'atteindre l'objectif de cette condition, à savoir empêcher des attaques. <p>Remarque : « L'entreprise spécialisée dans la sécurité des applications » peut être une société tierce ou une entité interne, l'essentiel étant que le personnel chargé de réaliser la vérification soit spécialisé dans la sécurité des applications et puisse attester de sa totale indépendance vis-à-vis de l'équipe de développement.</p>

Conditions PCI DSS	Procédures de test	Directive
<p>6.7 Assurer que les politiques de sécurité et les procédures opérationnelles pour le développement et la maintenance de la sécurité des systèmes et applications sont documentées, utilisées et connues de toutes les parties concernées.</p>	<p>6.7 Examiner la documentation et interroger le personnel pour vérifier que les politiques de sécurité et les procédures opérationnelles pour le développement et la maintenance de la sécurité des systèmes et des applications sont :</p> <ul style="list-style-type: none"> • Documentées, • Utilisées et • Connues de toutes les parties concernées. 	<p>Le personnel doit être conscient et suivre les politiques de sécurité et les procédures opérationnelles pour garantir que les systèmes et les applications sont développés de manière sécurisée et protégés des vulnérabilités sur une base continue.</p>

Mise en œuvre de mesures de contrôle d'accès strictes

Condition 7 : Restreindre l'accès aux données de titulaires de carte aux seuls individus qui doivent les connaître

Pour veiller à ce que les données stratégiques ne soient accessibles qu'au personnel autorisé, des systèmes et des processus doivent être mis en place pour restreindre l'accès à ces données aux seuls individus qui doivent les connaître et en fonction de leurs responsabilités professionnelles.

En d'autres termes, les droits d'accès ne sont accordés qu'au plus petit nombre de données nécessaires et en fonction des tâches à effectuer.

Conditions PCI DSS	Procédures de test	Directive
<p>7.1 Restreindre l'accès aux composants de système et aux données de titulaires de carte aux seuls individus qui doivent y accéder pour mener à bien leur travail.</p>	<p>7.1 Examiner la politique écrite de contrôle des accès et vérifier que la politique comprend les points 7.1.1 à 7.1.4 comme suit :</p> <ul style="list-style-type: none"> • Définir les besoins d'accès et les affectations de privilèges pour chaque rôle. • La restriction d'accès des ID utilisateurs privilégiés aux privilèges les plus faibles nécessaires pour la réalisation du travail • L'affectation d'accès basée sur la classification et la fonction professionnelles de chaque employé • L'approbation documentée (électroniquement ou par écrit) par les parties autorisées pour tous les accès, y compris la liste de tous les privilèges spécifiques approuvés. 	<p>Plus le nombre de personnes ayant accès aux données de titulaires de carte est élevé, plus il y a de risques que le compte d'un utilisateur soit utilisé de manière frauduleuse. Restreindre l'accès aux seuls individus qui ont une raison professionnelle légitime aide l'entreprise à prévenir la manipulation des données de titulaires de carte par des utilisateurs inexpérimentés ou malveillants.</p>
<p>7.1.1 Définir les besoins d'accès pour chaque rôle, y compris :</p> <ul style="list-style-type: none"> • Les composants de système et les ressources de données dont chaque rôle a besoin pour accéder aux fonctions de son poste ; • Le niveau de privilège requis (par exemple utilisateur, administrateur, etc.) pour accéder aux ressources. 	<p>7.1.1 Sélectionner un échantillon de rôles et vérifier que les besoins d'accès de chaque rôle sont définis et comprennent :</p> <ul style="list-style-type: none"> • Les composants de système et les ressources de données dont chaque rôle a besoin pour accéder aux fonctions de son poste ; • Identification des privilèges nécessaires pour chaque rôle à accomplir dans leur fonction professionnelle. 	<p>Afin de limiter l'accès aux données de titulaires de carte aux seuls individus qui ont besoin de cet accès, il est tout d'abord nécessaire de définir les besoins d'accès de chaque rôle (par exemple administrateur de système, personnel du centre d'appel, agent de magasin), les systèmes/dispositifs/données auxquels chaque rôle a besoin d'accéder et le niveau de privilège nécessaire à chaque rôle pour effectuer efficacement les tâches assignées. Une fois que les rôles et les besoins d'accès correspondant ont été définis, l'accès peut être accordé aux individus en fonction.</p>

Conditions PCI DSS	Procédures de test	Directive
<p>7.1.2 Restreindre l'accès des ID utilisateurs privilégiés aux privilèges les plus faibles nécessaires pour la réalisation du travail</p>	<p>7.1.2.a Interroger le personnel responsable de l'affectation des accès pour vérifier que l'accès aux ID utilisateurs privilégiés est :</p> <ul style="list-style-type: none"> • Uniquement affecté aux rôles qui nécessitent spécifiquement ce type d'accès privilégié • Restreints aux privilèges les plus faibles nécessaires pour la réalisation du travail <p>7.1.2.b Sélectionner un échantillon d'ID utilisateur avec accès privilégié et interroger le personnel de direction responsable pour vérifier que les privilèges assignés sont :</p> <ul style="list-style-type: none"> • Nécessaires pour les fonctions du travail de cette personne • Restreints aux privilèges les plus faibles nécessaires pour la réalisation du travail 	<p>Lors de l'affectation d'ID privilégiée, il est important d'affecter uniquement les privilèges dont les individus ont besoin pour accomplir leur travail (le « moins de privilèges »). Par exemple, l'administrateur de base de données ou l'administrateur de sauvegarde ne doivent pas bénéficier des mêmes privilèges que l'administrateur du système global.</p> <p style="text-align: right;"><i>(suite à la page suivante)</i></p> <p>L'affectation du moins de privilèges possibles aide à empêcher les utilisateurs qui ne connaissent pas suffisamment l'application de modifier sa configuration accidentellement ou de manière incorrecte, ou de modifier ses réglages de sécurité. Appliquer le moins de privilèges aide à minimiser la portée des dommages si une personne non autorisée obtient l'accès à un ID utilisateur.</p>
<p>7.1.3 Affecter l'accès basé sur la classification et la fonction professionnelles de chaque employé</p>	<p>7.1.3 Sélectionner un échantillon d'ID utilisateur et interroger le personnel de direction responsable pour vérifier que les privilèges assignés sont basés sur la classification et la fonction professionnelles de cette personne.</p>	<p>Une fois que les besoins sont définis pour les rôles d'utilisateur (selon la condition 7.1.1 de la norme PCI DSS), il est facile d'attribuer les droits d'accès individuels en fonction de la classification et de la fonction professionnelles en utilisant les rôles déjà créés.</p>
<p>7.1.4 Demander l'approbation documentée des parties responsables spécifiant les privilèges requis.</p>	<p>7.1.4 Sélectionner un échantillon d'ID utilisateur et comparer avec les approbations documentées pour vérifier que :</p> <ul style="list-style-type: none"> • L'approbation documentée existe pour les privilèges assignés ; • L'approbation provenait des parties autorisées ; • Que les privilèges spécifiques correspondent aux rôles affectés à l'individu. 	<p>Les approbations documentées (par exemple, par écrit ou électroniquement) assurent que ceux qui détiennent ces accès et ces privilèges sont connus et autorisés par la direction et que leur accès est nécessaire pour l'accomplissement de leur fonction professionnelle.</p>

Conditions PCI DSS	Procédures de test	Directive
<p>7.2 Établir des systèmes de contrôle d'accès pour les composants de système qui limitent l'accès aux seuls utilisateurs qui doivent accéder aux données et qui est configuré pour « refuser tous les accès » à moins qu'ils ne soient explicitement autorisés.</p> <p>Ces systèmes de contrôle d'accès doivent inclure les éléments suivants :</p>	<p>7.2 Examiner les paramètres du système et la documentation du fournisseur pour vérifier que les systèmes de contrôle d'accès sont déployés comme suit :</p>	<p>Sans un mécanisme de restriction de l'accès en fonction du besoin d'en connaître d'un utilisateur, celui-ci peut, sans le savoir, se voir accorder l'accès aux données de titulaires de carte. Les systèmes de contrôle d'accès automatisent le processus de restriction d'accès et l'affectation de privilèges. De plus, un réglage « tout refuser » par défaut assure que personne ne puisse obtenir l'accès à moins qu'une règle établie spécialement n'accorde cet accès. Les entités peuvent avoir un ou plusieurs systèmes de contrôle d'accès pour gérer l'accès des utilisateurs.</p>
<p>7.2.1 Couverture de tous les composants de système</p>	<p>7.2.1 Confirmer que les systèmes de contrôle d'accès sont en place sur tous les composants de système.</p>	<p>Remarque : Sur certains systèmes de contrôle d'accès, le paramètre « Autoriser tout » est configuré par défaut. Par conséquent, l'accès est autorisé à tous, à moins qu'une règle écrite ne précise explicitement le refus de l'accès.</p>
<p>7.2.2 L'octroi de privilèges aux individus repose sur leur classification et leur fonction professionnelles.</p>	<p>7.2.2 Confirmer que les systèmes de contrôle d'accès sont configurés pour octroyer les privilèges aux individus en fonction de leur classification et fonctions professionnelles.</p>	
<p>7.2.3 Configuration par défaut du paramètre « Refuser tout ».</p>	<p>7.2.3 Confirmer que les systèmes de contrôle d'accès intègrent un paramètre par défaut « Refuser tout ».</p>	
<p>7.3 Assurer que les politiques de sécurité et les procédures opérationnelles pour la restriction de l'accès aux données de titulaires de carte sont documentées, utilisées et connues de toutes les parties concernées.</p>	<p>7.3 Examiner la documentation et interroger le personnel pour vérifier que les politiques de sécurité et les procédures opérationnelles pour la restriction de l'accès aux données de titulaires de carte sont :</p> <ul style="list-style-type: none"> • Documentées • Utilisées et • Connues de toutes les parties concernées. 	<p>Le personnel doit être conscient et suivre les politiques de sécurité et les procédures opérationnelles pour garantir que l'accès est contrôlé et basé sur le besoin de savoir et le moins de privilèges sur une base continue.</p>

Condition 8 : Identifier et authentifier l'accès aux composants de système

En affectant un identifiant (ID) unique à chaque personne ayant un accès, on s'assure que chaque individu sera personnellement responsable de ses actes. Lorsque cette responsabilité est en place, les actions prises sur des données et des systèmes stratégiques sont effectuées par, et peuvent être retracées, des utilisateurs et des processus connus et autorisés.

L'efficacité d'un mot de passe est fortement déterminée par la conception et l'implémentation du système d'authentification, particulièrement, la fréquence avec laquelle les tentatives de mot de passe peuvent être faites par un pirate et les méthodes de sécurité utilisées pour protéger les mots de passe au point d'entrée, pendant la transmission et le stockage.

Remarque : Ces obligations concernent tous les comptes, y compris ceux des points de vente, avec une capacité administrative, et tous les comptes utilisés pour voir ou accéder aux données de titulaires de carte ou pour accéder à des systèmes comportant ce type de données. Ceux-ci comprennent les comptes utilisés par les fournisseurs et les autres tiers (par exemple, pour l'assistance ou l'entretien) Ces conditions ne s'appliquent pas aux comptes utilisés par les consommateurs (comme les titulaires de cartes).

Cependant, les conditions 8.1.1, 8.2, 8.5, 8.2.3 à 8.2.5 et 8.1.6 à 8.1.8 ne sont pas destinées aux comptes utilisateurs au sein d'une application de paiement de point de vente, qui n'ont accès qu'à un numéro de carte à la fois afin de permettre une transaction unique (comme les comptes de caisse).

Conditions PCI DSS	Procédures de test	Directive
<p>8.1 Définir et mettre en œuvre des politiques et des procédures pour assurer la gestion appropriée de l'identification des utilisateurs pour les utilisateurs non consommateurs et pour les administrateurs sur tous les composants de système comme suit :</p>	<p>8.1.a Examiner les procédures et confirmer qu'elles définissent les processus pour chacun des éléments ci-dessous de 8.1.1 à 8.1.8</p> <p>8.1.b Vérifier que les procédures sont mises en œuvre pour la gestion de l'identification des utilisateurs, en accomplissant ce qui suit :</p>	<p>En s'assurant que chaque utilisateur est identifié de manière unique, au lieu d'utiliser un ID unique pour plusieurs employés, une entreprise peut gérer la responsabilité des actes de chaque individu et effectuer une vérification à rebours efficace par employé. Cela accélérera la résolution des problèmes et en limitera les conséquences en cas d'erreur ou d'intentions malveillantes.</p>
<p>8.1.1 Affecter à tous les utilisateurs un ID unique avant de les autoriser à accéder à des composants de système ou aux données de titulaires de carte.</p>	<p>8.1.1 Interroger le personnel administratif pour confirmer que tous les utilisateurs ont un ID unique pour accéder aux composants de système ou aux données de titulaires de carte.</p>	
<p>8.1.2 Contrôler l'ajout, la suppression et la modification d'ID d'utilisateur, d'informations d'identification et d'autres objets identifiant.</p>	<p>8.1.2 Pour un échantillon d'ID d'utilisateur privilégiés et d'ID d'utilisateur génériques, examiner les autorisations associées et observer les réglages de système pour vérifier que chaque ID utilisateur et chaque ID utilisateur privilégié a été mise en œuvre avec seulement les privilèges spécifiés sur l'approbation documentée.</p>	

Conditions PCI DSS	Procédures de test	Directive
<p>8.1.3 Révoquer immédiatement l'accès de tout utilisateur qui ne travaille plus pour la société.</p>	<p>8.1.3.a Sélectionner un échantillon d'employés qui ont quitté la société au cours des six derniers mois, et passer en revue les listes d'accès pour examiner à la fois l'accès local et l'accès distant, afin de vérifier que leur ID ont été désactivées ou supprimées de la liste d'accès.</p> <p>8.1.3.b Vérifier que toutes les méthodes d'authentification physiques, telles que les cartes électroniques, jetons, etc., ont été rendues ou désactivées.</p>	<p>Si un employé a quitté la société et a toujours accès au réseau par son compte d'utilisateur, des accès inutiles ou malveillants aux données de titulaires de carte pourraient se produire, soit par un ancien employé soit par un individu malveillant qui exploite le vieux compte inutilisé. Pour empêcher les accès non autorisés, les justificatifs d'utilisateur et les autres méthodes d'authentification doivent donc être révoqués rapidement (dès que possible) après le départ d'un employé.</p>
<p>8.1.4 Supprimer/Désactiver les comptes d'utilisateur inactifs dans un délai de 90 jours.</p>	<p>8.1.4 Observer les comptes utilisateur pour vérifier que les comptes inactifs depuis plus de 90 jours sont supprimés ou désactivés.</p>	<p>Les comptes qui ne sont pas utilisés régulièrement sont souvent les cibles d'attaques puisqu'il est moins probable que les modifications (comme les changements de mot de passe) soient remarquées. Ainsi, ces comptes seront plus facilement exploités et utilisés pour accéder aux données de titulaires de carte.</p>
<p>8.1.5 Gérer les ID utilisés par les parties tierces pour accéder, prendre en charge ou maintenir les composants de système par accès à distance comme suit :</p> <ul style="list-style-type: none"> • Activés uniquement pendant la période de temps nécessaire et désactivés lorsqu'ils ne sont pas utilisés. • Surveillés lorsqu'ils sont utilisés. 	<p>8.1.5.a Interroger le personnel et observer les processus de gestion des comptes utilisés par les parties tierces pour accéder, prendre en charge ou maintenir les composants de système pour vérifier que les comptes utilisés pour l'accès à distance sont :</p> <ul style="list-style-type: none"> • Désactivés lorsqu'ils ne sont pas utilisés. • Activés uniquement lorsqu'ils sont nécessaires pour la partie tierce et désactivés lorsqu'ils ne sont pas utilisés. <p>8.1.5.b Interroger le personnel et observer les processus pour vérifier que les comptes d'accès à distance de la partie tierce sont contrôlés pendant leur utilisation.</p>	<p>Autoriser les fournisseurs à accéder à un réseau 24h/24 et 7 jours sur 7 au cas où ils auraient besoin d'intervenir sur les systèmes, augmente les risques d'accès non autorisé, de la part d'un utilisateur, appartenant à l'environnement du fournisseur ou d'un individu malveillant, qui découvre et exploite ce point d'entrée toujours disponible sur le réseau. Permettre l'accès uniquement pour la période de temps nécessaire et le désactiver dès qu'il n'est plus nécessaire aide à empêcher les utilisations malveillantes de ces connexions.</p> <p>La surveillance des accès de fournisseur donne l'assurance que les fournisseurs accèdent uniquement aux systèmes nécessaires, et uniquement pendant les périodes de temps approuvées.</p>
<p>8.1.6 Limiter les tentatives d'accès répétées en verrouillant l'ID d'utilisateur après six tentatives au</p>	<p>8.1.6.a Pour un échantillon de composants de système, inspecter les réglages de configuration pour vérifier que les paramètres d'authentification sont configurés pour exiger le verrouillage d'un compte d'utilisateur après six tentatives de</p>	<p>Sans des mécanismes de blocage de compte, un pirate peut en permanence tenter de deviner un mot de passe à l'aide d'outils manuels ou automatiques (par exemple, craquage de mots de passe), jusqu'à</p>

Conditions PCI DSS	Procédures de test	Directive
maximum.	<p>connexion non valides au maximum.</p> <p>8.1.6.b Procédure de tests supplémentaires pour évaluer les prestataires de services uniquement : Examiner les processus internes et la documentation des clients/utilisateurs et observer les processus mis en œuvre pour vérifier que les comptes des utilisateurs clients non consommateurs sont provisoirement verrouillés après six tentatives d'accès non valides, tout au plus.</p>	<p>ce qu'il réussisse et l'utilise pour accéder au compte d'un utilisateur.</p> <p>Remarque : La procédure de test 8.1.6.b est une procédure supplémentaire qui s'applique uniquement si l'entité en cours d'évaluation est un prestataire de services.</p>
<p>8.1.7 Régler la durée de verrouillage sur 30 minutes au minimum ou jusqu'à ce que l'administrateur active l'ID d'utilisateur.</p>	<p>8.1.7 Pour un échantillon de composants de système, inspecter les paramètres de configuration du système pour vérifier que les mots de passe sont configurés pour exiger qu'un compte d'utilisateur, une fois verrouillé, reste à cet état 30 minutes au moins ou jusqu'à ce qu'un administrateur système réinitialise le compte.</p>	<p>Si un compte est bloqué parce que quelqu'un a essayé à plusieurs reprises d'en deviner le mot de passe, des contrôles retardant la réactivation de ce compte empêchent l'individu malveillant de poursuivre (il devra s'arrêter pendant au moins 30 minutes jusqu'à la réactivation du compte). De plus, si la réactivation doit être demandée, l'administrateur ou le bureau d'aide peuvent valider qu'il s'agit bien du propriétaire du compte qui demande sa réactivation.</p>
<p>8.1.8 Si une session reste inactive pendant plus de 15 minutes, demander à l'utilisateur de s'authentifier de nouveau pour réactiver le terminal ou la session.</p>	<p>8.1.8 Pour un échantillon de composants de système, inspecter les paramètres de configuration du système pour vérifier que les fonctions d'expiration du système/de la session sont réglées sur 15 minutes ou moins.</p>	<p>Lorsque les utilisateurs s'éloignent de leur ordinateur allumé ayant accès au réseau critique ou aux données de titulaires de carte, cette machine peut être utilisée par d'autres en l'absence de l'utilisateur pour accéder sans autorisation à un compte et/ou l'utiliser à des fins frauduleuses.</p> <p>La réauthentification peut être appliquée au niveau du système pour protéger toutes les sessions en cours sur cette machine, ou au niveau de l'application.</p>

Conditions PCI DSS	Procédures de test	Directive
<p>8.2 En plus de l'affectation d'un ID unique, s'assurer qu'une gestion appropriée des mots de passe et de l'authentification des utilisateurs est mise en œuvre pour les utilisateurs non-consommateurs et les administrateurs sur tous les composants de système en employant au moins une des méthodes suivantes pour identifier tous les utilisateurs :</p> <ul style="list-style-type: none"> • Quelque chose de connu du seul utilisateur, comme un mot de passe ou une locution de passage ; • Quelque chose de détenu par l'utilisateur, comme un dispositif de jeton ou une carte à puce ; • Quelque chose que vous détenez, comme une mesure biométrique. 	<p>8.2 Pour vérifier que les utilisateurs sont authentifiés à l'aide d'un ID unique et une autre méthode d'authentification (par exemple, un mot/phrase de passe) pour accéder à l'environnement des données de titulaires de carte, procéder comme suit :</p> <ul style="list-style-type: none"> • Examiner la documentation qui décrit les méthodes d'authentification utilisées. • Pour chaque type de méthode d'authentification employée et pour chaque type de composant du système, observer une authentification pour vérifier qu'elle se déroule conformément aux méthodes d'authentification décrites. 	<p>Ces méthodes d'authentification, lorsqu'elles sont utilisées en plus des ID uniques, protègent les ID uniques des utilisateurs et évitent qu'ils ne soient compromis, puisque la personne qui en est responsable de cette tentative doit connaître l'ID unique et le mot de passe (ou tout autre élément d'authentification utilisé). Remarque qu'un certificat numérique est une option valable comme forme d'authentification du type « quelque chose de détenu », tant qu'il reste unique pour un utilisateur spécifique.</p> <p>Dans la mesure où l'une des premières mesures qu'un individu malveillant prendra pour compromettre un système étant d'exploiter la faiblesse ou l'absence de mots de passe, il est important de mettre en place des processus appropriés pour la gestion de l'authentification.</p>

Conditions PCI DSS	Procédures de test	Directive
<p>8.2.1 Utiliser une cryptographie robuste, rendre tous les justificatifs d'authentification (tels que les mots/phrases de passe) illisibles pendant la transmission et le stockage sur tous les composants de système.</p>	<p>8.2.1.a Examiner la documentation du fournisseur et les réglages de configuration du système pour vérifier que les mots de passe sont protégés avec une cryptographie robuste pendant la transmission et le stockage.</p>	<p>De nombreux dispositifs et applications réseau transmettent des mots de passe non cryptés et lisibles sur le réseau et/ou stockent les mots de passe sans cryptage. Un individu malveillant peut facilement intercepter les mots de passe non cryptés durant leur transmission à l'aide d'un « renifleur », ou accéder directement aux mots de passe non cryptés, dans les fichiers où ils sont stockés et utiliser ces données pour accéder sans autorisation au réseau.</p> <p><i>Remarque : Les procédures de test 8.2.1.d et 8.2.1.e sont des procédures supplémentaires, qui s'appliquent uniquement si l'entité en cours d'évaluation est un prestataire de services.</i></p>
	<p>8.2.1.b Pour un échantillon de composants de système, examiner les fichiers de mots de passe pour vérifier que les mots de passe sont illisibles pendant le stockage.</p>	
	<p>8.2.1.c Pour un échantillon de composants de système, examiner les transmissions de données pour vérifier que les mots de passe sont illisibles pendant la transmission.</p>	
	<p>8.2.1.d Procédure de tests supplémentaires pour évaluer les prestataires de services uniquement : Observer les fichiers de mots de passe pour vérifier que les mots de passe des clients non consommateurs sont illisibles pendant le stockage.</p>	
	<p>8.2.1.e Procédure de tests supplémentaires pour évaluer les prestataires de services uniquement : Observer les transmissions de données pour vérifier que les mots de passe des clients non consommateurs sont illisibles pendant la transmission.</p>	
<p>8.2.2 Vérifier l'identité de l'utilisateur avant de modifier tout justificatif d'authentification, par exemple, lors des réinitialisations de mot de passe, la délivrance de nouveaux jetons ou la création de nouvelles clés.</p>	<p>8.2.2 Examiner les procédures d'authentification pour modifier les justificatifs d'authentification et observer le personnel en charge de la sécurité pour vérifier que, si un utilisateur demande la réinitialisation de son mot de passe par téléphone, par e-mail, via Internet ou toute autre méthode n'impliquant pas un face-à-face, que son identité est vérifiée avant la modification du justificatif d'authentification.</p>	<p>De nombreux individus malveillants utilisent « l'ingénierie sociale », par exemple en appelant un service d'assistance et en agissant comme un utilisateur légitime, afin d'obtenir un changement de mot de passe de sorte qu'ils puissent utiliser un ID utilisateur. Envisager l'utilisation d'une « question secrète » à laquelle seul le vrai utilisateur peut répondre, afin d'aider les administrateurs à identifier l'utilisateur avant de reconfigurer ou de modifier les justificatifs d'authentification.</p>

Conditions PCI DSS	Procédures de test	Directive
<p>8.2.3 Les mots de passe/locutions de passage doivent respecter les critères suivants :</p> <ul style="list-style-type: none"> • Exiger une longueur minimale d'au moins sept caractères ; • Comporter à la fois des caractères numériques et des caractères alphabétiques. <p>Autrement, les mots de passe/locutions de passage doivent avoir une complexité et une puissance au moins équivalentes aux paramètres spécifiés ci-dessus.</p>	<p>8.2.3.a Pour un échantillon de composants de système, inspecter les paramètres de configuration du système pour vérifier que les paramètres de mot de passe/locution de passage utilisateur sont configurés de manière à exiger au moins la robustesse/complexité suivante :</p> <ul style="list-style-type: none"> • Exiger une longueur minimale d'au moins sept caractères ; • Comporter à la fois des caractères numériques et des caractères alphabétiques. <p>8.2.3.b Procédure de tests supplémentaires pour évaluer les prestataires de services uniquement : Examiner les processus internes et la documentation des clients/utilisateurs pour vérifier qu'il est demandé aux clients non consommateurs de définir des mots de passe/locutions de passage d'une robustesse/complexité respectant au moins les critères suivants :</p> <ul style="list-style-type: none"> • Exiger une longueur minimale d'au moins sept caractères ; • Comporter à la fois des caractères numériques et des caractères alphabétiques. 	<p>Des mots de passe/locutions de passage robustes sont la première ligne de défense d'un réseau, puisque les individus malveillants rechercheront souvent d'abord les comptes dont les mots de passe sont faibles ou inexistantes. Si les mots de passe sont courts, faciles à deviner il est relativement facile pour un individu malveillant de découvrir ces comptes faibles et de compromettre un réseau sous couvert d'un ID utilisateur valide.</p> <p>Cette condition spécifie que les mots de passe/locutions de passage doivent être d'une longueur minimum de sept caractères et utiliser à la fois des caractères numériques et des caractères alphabétiques. Pour les cas où ce minimum ne peut pas être respecté en raison de limitations techniques, les entités peuvent utiliser une « force équivalente » pour évaluer leur alternative. Pour plus d'informations sur la variabilité et l'équivalence de la robustesse (aussi appelée « entropie ») pour les mots de passe/locutions de passage sous divers formats, se reporter aux normes sectorielles (comme la version actuelle de NIST SP 800-63).</p> <p>Remarque : La procédure de test 8.2.3.b est une procédure supplémentaire qui s'applique uniquement si l'entité en cours d'évaluation est un prestataire de services.</p>
<p>8.2.4 Modifier les mots de passe/locutions de passage utilisateur au moins tous les 90 jours.</p>	<p>8.2.4.a Pour un échantillon de composants de système, inspecter les paramètres de configuration système pour vérifier que les paramètres de mots de passe/locutions de passage utilisateur sont configurés de manière à demander aux utilisateurs de modifier leurs mots de passe au moins tous les 90 jours.</p> <p>8.2.4.b Procédure de tests supplémentaires pour évaluer les prestataires de services uniquement : Examiner les processus internes et la documentation de client/utilisateur pour vérifier que :</p> <ul style="list-style-type: none"> • Les mots de passe/locutions de passage des utilisateurs 	<p>Les mots de passe/locutions de passage qui sont valides sur une longue période sans être changés donnent aux individus malveillants plus de temps pour les décoder.</p> <p>Remarque : La procédure de test 8.2.4.b est une procédure supplémentaire qui s'applique uniquement si l'entité en cours d'évaluation est un prestataire de services.</p>

Conditions PCI DSS	Procédures de test	Directive
	<p>clients non consommateurs doivent changer régulièrement et</p> <ul style="list-style-type: none"> Les utilisateurs clients non consommateurs sont guidés quant au moment et aux circonstances dans lesquelles les mots de passe/locutions de passage doivent être changés. 	
<p>8.2.5 Interdire à un individu de soumettre un nouveau mot de passe/locution de passage identique à l'un de quatre derniers mots de passe/locutions de passage utilisés.</p>	<p>8.2.5.a Pour un échantillon de composants de système, obtenir et inspecter les paramètres de configuration du système pour vérifier que les paramètres de mot de passe sont configurés pour exiger que les nouveaux mots de passe/locutions de passage ne puissent pas être les mêmes que les quatre derniers.</p> <p>8.2.5.b Procédure de tests supplémentaires pour évaluer les prestataires de services uniquement : Examiner les processus internes et la documentation des clients/utilisateurs pour vérifier que les nouveaux mots de passe/locutions de passage des utilisateurs clients non consommateurs ne puissent pas être identiques aux quatre derniers.</p>	<p>Si l'historique de mot de passe n'est pas maintenu, l'efficacité du changement de mot de passe est réduite, dans la mesure où il est possible de réutiliser indéfiniment les mots de passe précédents. Demander à ce que les mots de passe ne puissent pas être réutilisés pendant une certaine période de temps réduit la possibilité que des mots de passe qui ont été devinés ou forcés soient utilisés à l'avenir.</p> <p><i>Remarque : La procédure de test 8.2.5.b est une procédure supplémentaire qui s'applique uniquement si l'entité en cours d'évaluation est un prestataire de services.</i></p>
<p>8.2.6 Définir des mots de passe/locutions de passage pour la première utilisation et suite à la réinitialisation pour une valeur unique pour chaque utilisateur et changer immédiatement après la première utilisation.</p>	<p>8.2.6 Examiner les procédures relatives aux mots de passe et observer le personnel chargé de la sécurité pour vérifier que les mots de passe/locutions de passage initiaux pour chaque nouvel utilisateur, et les mots de passe/locutions de passage réinitialisés pour les utilisateurs existants sont configurés sur une valeur unique à chaque utilisateur et qu'ils sont modifiés après leur première utilisation.</p>	<p>Si le même mot de passe est utilisé pour chaque nouvel utilisateur, un utilisateur interne, un ancien employé ou un individu malveillant peuvent connaître ou facilement découvrir ce mot de passe et l'utiliser pour accéder aux comptes.</p>

Conditions PCI DSS	Procédures de test	Directive
<p>8.3 Sécuriser tous les accès administratifs non-console et tous les accès distants au CDE par authentification à plusieurs facteurs.</p> <p>Remarque : L'authentification à plusieurs facteurs requiert d'utiliser au moins deux des trois méthodes d'authentification (voir la condition 8.2 pour les descriptions des méthodes d'authentification). L'utilisation à deux reprises d'un facteur (par exemple, l'utilisation de deux mots de passe distincts) ne constitue pas une authentification à plusieurs facteurs.</p>		<p>L'authentification à plusieurs facteurs exige qu'un individu présente au moins deux formes distinctes d'authentification (comme décrit dans la condition 8.2) avant qu'il puisse recevoir son droit d'accès.</p> <p>L'authentification à plusieurs facteurs octroie une assurance supplémentaire dans la mesure où l'individu tentant un accès doit correspondre à la personne qu'il prétend être. Grâce à une authentification à plusieurs facteurs, une personne malveillante doit compromettre au moins deux mécanismes d'authentification, ce qui augmente la difficulté de violation de sécurité et réduit donc le risque.</p> <p>L'authentification à plusieurs facteurs n'est pas requise au niveau du système et au niveau de l'application pour un composant de système donné. Une authentification à plusieurs facteurs peut survenir lors de l'authentification pour accéder à un réseau donné ou à un composant de système donné.</p> <p>Les exemples de technologies à plusieurs facteurs comprennent, mais sans s'y limiter, l'authentification à distance et le service de renseignements par téléphone (remote authentication and dial-in service, RADIUS) avec jetons ; le système de contrôle d'accès au contrôleur d'accès du terminal (terminal access controller access control system, TACACS) avec jetons et les autres technologies permettant une authentification à plusieurs facteurs.</p>

Conditions PCI DSS	Procédures de test	Directive
<p>8.3.1 Incorporer l'authentification à plusieurs facteurs pour tous les accès non-console dans CDE pour les membres du personnel dotés d'un accès administratif.</p> <p><i>Remarque : Cette condition est considérée comme une meilleure pratique jusqu'au 31 janvier 2018, après quoi ce sera une obligation.</i></p>	<p>8.3.1.a Examiner les configurations réseau et/ou système, le cas échéant, pour vérifier si l'authentification à plusieurs facteurs est requise pour tous les accès administratifs non-console au CDE.</p> <p>8.3.1.b Observer un échantillon du personnel administratif qui se connecte au CDE et vérifier qu'au moins deux des trois méthodes d'authentification sont utilisées.</p>	<p>Cette condition est destinée à être appliquée à tout le personnel doté d'un accès administratif au CDE. Cette condition s'applique uniquement au personnel doté d'un accès administratif et d'un accès non-console au CDE. Elle ne s'applique pas aux comptes de l'application ou du système qui effectuent des fonctions automatisées.</p> <p>Si l'entité n'utilise pas la segmentation pour séparer le CDE du reste de son réseau, un administrateur peut recourir à l'authentification à plusieurs facteurs lors de la connexion au réseau CDE ou à un système.</p> <p>Si le CDE est segmenté du reste du réseau de l'entité, un administrateur doit recourir à l'authentification à plusieurs facteurs lors de la connexion à un système CDE ou à un autre réseau non CDE. L'authentification à plusieurs facteurs peut être implémentée au niveau du réseau ou du système/de l'application. Les deux ne sont pas obligatoires. Si l'administrateur a recours à l'authentification à plusieurs facteurs lors de la connexion au réseau CDE, il n'est pas tenu de l'utiliser pour se connecter à un système ou à une application donné(e) dans le CDE.</p>
<p>8.3.2 Incorporer une authentification à plusieurs facteurs pour tous les accès réseau à distance (utilisateur et administrateur, y compris l'accès des parties tierces dans un souci d'assistance ou de maintenance) provenant de l'extérieur du réseau de l'entité.</p>	<p>8.3.2.a Examiner les configurations du système pour les systèmes et les serveurs d'accès à distance afin de vérifier que l'authentification à plusieurs facteurs est requise pour :</p> <ul style="list-style-type: none"> • Tous les accès à distance par le personnel, que ce soit l'utilisateur ou l'administrateur, et • Tous les accès à distance de tiers/fournisseur (y compris les accès aux composants et systèmes des applications à fin d'assistance ou de maintenance). <p>8.3.2.b Observer un échantillon du personnel (par exemple les utilisateurs et les administrateurs) qui se connecte à distance au réseau et vérifier qu'au moins deux des trois méthodes d'authentification sont utilisées.</p>	<p>Cette condition est destinée à être appliquée à tout le personnel, y compris les utilisateurs généraux, les administrateurs et les fournisseurs (dans un souci d'assistance ou de maintenance) ayant un accès à distance au réseau, lorsque cet accès à distance peut permettre de pénétrer dans le CDE. Si un accès à distance s'effectue vers le réseau d'une entité possédant une segmentation appropriée, ces utilisateurs à distance ne peuvent ni accéder ni affecter l'environnement des données de titulaires de carte et une authentification à plusieurs facteurs pour l'accès à distance à ce réseau ne sera pas exigée. Cependant, l'authentification à plusieurs</p>

Conditions PCI DSS	Procédures de test	Directive
<p>8.4 Documenter et communiquer les politiques et les procédures d'authentification à tous les utilisateurs, y compris :</p> <ul style="list-style-type: none"> • Des directives concernant la sélection de justificatifs d'authentification robustes ; • Des directives expliquant comment les utilisateurs doivent protéger leurs justificatifs d'authentification ; • Des instructions stipulant qu'il ne faut pas réutiliser les mots de passe ayant déjà été utilisés ; • Des instructions expliquant comment changer les mots de passe si l'on soupçonne que le mot de passe est compromis. 	<p>8.4.a Examiner les procédures et interroger le personnel pour vérifier que les politiques et procédures d'authentification sont distribuées à tous les utilisateurs.</p> <p>8.4.b Examiner les politiques et les procédures d'authentification qui sont distribuées aux utilisateurs et vérifier qu'elles comprennent :</p> <ul style="list-style-type: none"> • Des directives concernant la sélection de justificatifs d'authentification robustes ; • Des directives expliquant comment les utilisateurs doivent protéger leurs justificatifs d'authentification ; • Des instructions stipulant que les utilisateurs ne doivent pas réutiliser les mots de passe ayant déjà été utilisés ; • Des instructions expliquant comment changer les mots de passe si l'on soupçonne que le mot de passe est compromis. <p>8.4.c Interroger un échantillon d'utilisateurs pour vérifier qu'ils connaissent les politiques et les procédures d'authentification.</p>	<p>facteurs est exigée pour tout accès à distance à des réseaux ayant eux-mêmes accès à l'environnement des données de titulaires de carte. Elle est recommandée pour tout accès à distance aux réseaux de l'entité.</p> <p>La communication des politiques et des procédures de mot de passe/authentification à tous les utilisateurs permet à ces utilisateurs de comprendre et de respecter les politiques.</p> <p>Par exemple, les directives sur la sélection de mots de passe robustes peuvent inclure des suggestions pour aider le personnel à sélectionner des mots de passe difficiles à deviner qui ne contiennent pas de mots du dictionnaire et qui ne contiennent pas d'informations concernant l'utilisateur (telles que l'ID utilisateur, les noms de membres de sa famille, date de naissance, etc.). Les directives pour la protection des justificatifs d'authentification peuvent inclure l'interdiction d'écrire les mots de passe ou de les enregistrer dans des fichiers non sécurisés, et ainsi que de rester vigilants au cas où un individu malveillant tenterait d'exploiter leurs mots de passe (par exemple, en appelant un employé pour lui demander son mot de passe en vue de « résoudre un problème »).</p> <p>Demander aux utilisateurs de changer leur mot de passe s'il existe une possibilité que le mot de passe ne soit plus sécurisé peut empêcher aux utilisateurs malveillants d'utiliser un mot de passe légitime pour obtenir un accès non autorisé.</p>
<p>8.5 Ne pas utiliser de méthode d'authentification par groupe, partagé ou de mots de passe d'ID génériques comme suit :</p> <ul style="list-style-type: none"> • Les ID d'utilisateur génériques sont désactivés ou supprimés. • Les ID d'utilisateur partagés n'existent pas pour les fonctions 	<p>8.5.a Pour un échantillon de composants de système, examiner les listes d'ID d'utilisateur pour vérifier les points suivants :</p> <ul style="list-style-type: none"> • Les ID d'utilisateur génériques sont désactivés ou supprimés. • Il n'existe pas d'ID d'utilisateur partagé pour les activités d'administration du système et d'autres fonctions stratégiques ; • Aucun ID d'utilisateur partagé ou générique n'est utilisé pour l'administration du moindre composant du système. 	<p>Si plusieurs utilisateurs partagent les mêmes justificatifs d'authentification (par exemple, le même compte utilisateur et le même mot de passe), il devient impossible de retracer l'accès au système et les activités jusqu'à un individu. Cette caractéristique empêche à une entité de déterminer les responsabilités ou d'avoir un journal efficace des actions individuelles, dans la mesure où une action</p>

Conditions PCI DSS	Procédures de test	Directive
<p>d'administration du système et les autres fonctions critiques.</p> <ul style="list-style-type: none"> Aucun ID d'utilisateur partagé ou générique n'est utilisé pour l'administration du moindre composant du système. 	<p>8.5.b Examiner les politiques et les procédures d'authentification pour vérifier que le recours aux ID collectifs et partagés et/ou aux mots de passe ou autres méthodes d'authentification est interdit de façon explicite.</p> <p>8.5.c Interroger les administrateurs système pour vérifier que les ID et/ou mots de passe ou autre méthode d'authentification de groupes et partagés ne sont pas distribuées, même en cas de demande.</p>	<p>donnée pourrait avoir été accomplie par n'importe quelle personne du groupe ayant connaissance des justificatifs d'authentification.</p>
<p>8.5.1 Condition supplémentaire pour les prestataires de services uniquement : Les prestataires de services ayant un accès à distance aux installations des clients (par exemple, pour l'assistance des systèmes ou des serveurs de POS) doivent utiliser un justificatif d'authentification unique (tel qu'un mot/phrase de passe) pour chaque client.</p> <p><i>Remarque</i> : Cette condition n'est pas prévue pour s'appliquer aux fournisseurs d'hébergement partagé qui accèdent à leur propre environnement d'hébergement, où de multiples environnements de client sont hébergés.</p>	<p>8.5.1 Procédure de tests supplémentaires pour évaluer les prestataires de services uniquement : Examiner les politiques et les procédures d'authentification et interroger le personnel pour vérifier que différents justificatifs d'authentification sont utilisés pour accéder à chaque client.</p>	<p><i>Remarque</i> : Cette condition ne s'applique que lorsque l'entité évaluée est un prestataire de services.</p> <p>Pour empêcher que de multiples clients soient compromis en utilisant un seul ensemble de justificatifs, les fournisseurs ayant des comptes d'accès à distance aux environnements de client doivent utiliser un justificatif d'authentification différent pour chaque client.</p> <p>Les technologies, comme les mécanismes à plusieurs facteurs, qui donnent un justificatif unique pour chaque connexion (par exemple, au moyen d'un mot de passe unique) doivent également remplir l'objectif de cette condition.</p>

Conditions PCI DSS	Procédures de test	Directive
<p>8.6 Lorsque les autres mécanismes d'authentification sont utilisés (par exemple, des jetons de sécurité logiques ou physiques, des cartes électroniques, certificats, etc.) l'utilisation de ces mécanismes doit être assignée comme suit :</p> <ul style="list-style-type: none"> • Les mécanismes d'authentification doivent être affectés à un compte individuel et non pas partagés par de multiples comptes. • Les contrôles logiques et/ou physiques doivent être en place pour garantir que seul le compte prévu puisse utiliser ce mécanisme pour obtenir l'accès. 	<p>8.6.a Examiner les politiques et les procédures d'authentification pour vérifier que les procédures des mécanismes d'authentification, comme les jetons de sécurité physique, les cartes électroniques et les certificats, soient définis et comprennent :</p> <ul style="list-style-type: none"> • Les mécanismes d'authentification sont affectés à un compte individuel et non pas partagés par de multiples comptes. • Les contrôles logiques et/ou physiques sont définis pour garantir que seul le compte prévu puisse utiliser ce mécanisme pour obtenir l'accès. 	<p>Si les mécanismes d'authentification d'utilisateur, tels que les jetons, les cartes électroniques et les certificats, peuvent être utilisés par de multiples comptes, il pourrait être possible d'identifier l'individu qui utilise le mécanisme d'authentification. Appliquer des contrôles physiques et/ou logiques (par exemple un code PIN, des données biométriques ou un mot de passe) pour identifier de manière unique l'utilisateur du compte empêchera les utilisateurs non autorisés d'obtenir l'accès en utilisant un mécanisme d'authentification partagé.</p>
	<p>8.6.b Interroger le personnel en charge de la sécurité pour vérifier que les mécanismes d'authentification sont affectés à un compte et ne sont pas partagés par de multiples comptes.</p>	
	<p>8.6.c Examiner les réglages de configuration de système et/ou les contrôles physiques, s'il y a lieu, pour vérifier que les contrôles sont mis en œuvre pour garantir que seul le compte prévu puisse utiliser ce mécanisme pour obtenir l'accès.</p>	
<p>8.7 Tous les accès à n'importe quelle base de données contenant des données de titulaires de carte (y compris les accès par les applications, administrateurs et autres utilisateurs) est restreint comme suit :</p> <ul style="list-style-type: none"> • Tous les accès d'utilisateur, demandes d'utilisateur et actions d'utilisateur sur les bases de données ont lieu au moyen de méthodes de programmation. • Seuls administrateurs de bases de données ont la possibilité d'accéder directement aux bases de données ou d'effectuer des demandes sur les 	<p>8.7.a Examiner les paramètres de configuration de la base de données et de l'application, et vérifier que tous les utilisateurs s'authentifient avant d'y accéder.</p>	<p>Sans une authentification des utilisateurs pour accéder aux bases de données et aux applications, les risques d'accès non autorisés ou à des fins malveillantes augmentent et ceux-ci ne peuvent pas être consignés dans les journaux puisque l'utilisateur n'a pas été authentifié et, par conséquent, est inconnu du système. En outre, l'accès aux bases de données doit être autorisé par un programme seulement (par exemple, par le biais de procédures stockées), plutôt qu'un accès direct des utilisateurs finaux à la base de données (à l'exception des DBA, qui peuvent nécessiter un accès direct dans le cadre de leurs tâches administratives).</p>
	<p>8.7.b Examiner les paramètres de configuration de la base de données et de l'application pour vérifier que tous les accès d'utilisateurs aux bases de données, toutes les consultations et toutes les actions exécutées dans celles-ci (par exemple, déplacement, copie, suppression d'informations) s'effectuent exclusivement au moyen de méthodes programmées (par exemple, par le biais de procédures stockées).</p>	
	<p>8.7.c Examiner les paramètres de contrôle d'accès à la base de données et les paramètres de configuration de la base de données de l'application et vérifier que tous les accès directs aux bases de données et toutes les consultations sont restreintes</p>	

Conditions PCI DSS	Procédures de test	Directive
<p>bases de données.</p> <ul style="list-style-type: none"> Les ID d'application pour les applications de base de données peuvent uniquement être utilisés par les applications (et non par des utilisateurs individuels ou d'autres processus). 	<p>aux administrateurs de base de données.</p> <p>8.7.d Examiner les paramètres de contrôle d'accès à la base de données, les paramètres de configuration d'application de base de données et les ID de l'application connexe pour vérifier que les ID d'application peuvent uniquement être utilisées par les applications (et non par des utilisateurs individuels ou d'autres processus).</p>	
<p>8.8 Assurer que les politiques de sécurité et les procédures opérationnelles pour l'identification et l'authentification sont documentées, utilisées et connues de toutes les parties concernées.</p>	<p>8.8 Examiner la documentation et interroger le personnel pour vérifier que les politiques de sécurité et les procédures opérationnelles pour l'identification et l'authentification sont :</p> <ul style="list-style-type: none"> Documentées Utilisées et Connues de toutes les parties concernées. 	<p>Le personnel doit être conscient et suivre les politiques de sécurité et les procédures opérationnelles pour la gestion des identifications et des authentifications sur une base continue.</p>

Condition 9 : Restreindre l'accès physique aux données de titulaires de carte

Dans la mesure où tout accès physique à des données ou à des systèmes hébergeant des données de titulaires de carte permet à des individus d'accéder à des périphériques ou à des informations, et de supprimer des systèmes ou des copies papier, cet accès doit être restreint de façon appropriée. Dans le cadre de cette condition 9, le terme « personnel du site » désigne les employés à temps plein et à temps partiel, les intérimaires ainsi que les sous-traitants et les consultants qui « résident » sur le site de l'entité. Un « visiteur » est défini comme un fournisseur, l'hôte du personnel du site, le personnel de service ou tout individu présent au sein des locaux pendant une période courte, n'excédant généralement pas une journée. « Support » se rapporte à tout support papier ou électronique contenant des données de titulaires de carte.

Conditions PCI DSS	Procédures de test	Directive
<p>9.1 Utiliser des contrôles d'accès aux installations appropriés pour restreindre et surveiller l'accès physique aux systèmes installés dans l'environnement des données de titulaires de carte.</p>	<p>9.1 Vérifier que des contrôles de sécurité physiques sont en place dans chaque salle informatique, centre de données et autres zones physiques qui abritent des systèmes appartenant à l'environnement des données de titulaires de carte.</p> <ul style="list-style-type: none"> • Vérifier que l'accès est contrôlé par des lecteurs de badge et autres dispositifs tels que des badges autorisés, des clés et des cadenas. • Observer un administrateur système alors qu'il tente de se connecter aux consoles de systèmes choisis de façon aléatoire dans l'environnement des données de titulaires de carte, et vérifier que ces consoles sont « verrouillées » pour empêcher toute utilisation non autorisée. 	<p>Sans contrôles d'accès physiques, tels que des systèmes de badge et des contrôles de porte, les personnes non autorisées pourraient potentiellement accéder à l'installation pour voler, désactiver, perturber ou détruire des systèmes critiques et des données de titulaires de carte.</p> <p>Le blocage des écrans de connexion sur les consoles empêche les personnes non autorisées d'accéder aux informations sensibles, d'altérer les configurations de système, d'introduire des vulnérabilités dans le réseau ou de détruire des archives.</p>
<p>9.1.1 Installer des caméras vidéo ou des mécanismes de contrôle d'accès pour contrôler l'accès physique des</p>	<p>9.1.1.a Vérifier que des caméras vidéo ou des mécanismes de contrôle d'accès (ou les deux) sont en place pour contrôler les points d'entrée/de sortie dans les zones sensibles.</p>	<p>Lors des enquêtes sur les violations physiques, ces contrôles peuvent aider à identifier les individus qui accèdent physiquement aux zones</p>

Conditions PCI DSS	Procédures de test	Directive
<p>individus aux zones sensibles. Examiner les données enregistrées et les mettre en corrélation avec d'autres informations. Les conserver pendant trois mois au minimum, sauf stipulation contraire de la loi.</p> <p>Remarque : Par « zones sensibles », nous entendons tout centre de données, salle de serveur ou zone abritant des systèmes qui stockent, traitent ou transmettent des données de titulaires de carte. Cette définition exclut les zones face au public où seuls les terminaux de point de vente sont présents, tels que les zones de caisse dans un magasin.</p>	<p>9.1.1.b Vérifier que les caméras vidéo ou les mécanismes de contrôle d'accès (ou les deux) sont protégés contre la falsification ou la désactivation.</p>	<p>sensibles, ainsi que quand ils y entrent ou en sortent.</p> <p>Les personnes malveillantes qui cherchent à obtenir un accès physique aux zones sensibles essayeront souvent de désactiver ou de contourner les contrôles de surveillance. Pour protéger ces contrôles des manipulations malveillantes, les caméras vidéo doivent être placées hors de portée et/ou surveillées pour détecter toute manipulation indésirable. De même, les mécanismes de contrôle d'accès pourraient être surveillés ou être munis de protections physiques pour les empêcher d'être endommagés ou désactivés par des individus malveillants.</p> <p style="text-align: right;"><i>(suite à la page suivante)</i></p>
	<p>9.1.1.c Vérifier que les données des caméras vidéo et/ou autres mécanismes de contrôle d'accès sont examinées, et que les données sont conservées pendant au moins trois mois.</p>	<p>Les exemples de zones sensibles comprennent les salles des serveurs de base de données de l'entreprise, les bureaux d'arrière-salle d'un point de vente au détail contenant des données de titulaires de carte et les lieux de stockage d'un volume important de données de titulaires de carte. Les zones sensibles doivent être identifiées par chaque organisation pour garantir que les surveillances physiques appropriées sont mises en œuvre.</p>

Conditions PCI DSS	Procédures de test	Directive
<p>9.1.2 Mettre en œuvre des contrôles physiques et/ou logiques pour restreindre l'accès physique aux prises réseau accessibles au public.</p> <p><i>Par exemple, les prises de réseau situées dans les zones publiques et les zones accessibles aux visiteurs doivent être désactivées et uniquement activées lorsque l'accès au réseau est accepté de manière explicite. Autrement, des processus doivent être mis en œuvre pour assurer que les visiteurs sont accompagnés à tout moment dans les zones contenant des prises réseau actives.</i></p>	<p>9.1.2 Interroger le personnel responsable et observer les emplacements de prises réseau accessibles au public pour vérifier que des contrôles physiques et/ou logiques sont en place pour restreindre l'accès des prises réseau accessibles au public.</p>	<p>Restreindre l'accès aux prises réseau (ou aux ports réseau) empêchera les individus malveillants de se brancher aux prises réseau disponibles et d'accéder aux ressources des réseaux internes.</p> <p>Qu'il s'agisse de contrôles logiques ou physiques, ou d'une combinaison des deux, ces contrôles doivent être suffisants pour empêcher un individu ou un dispositif qui n'est pas explicitement autorisé de pouvoir se connecter au réseau.</p>
<p>9.1.3 Restreindre l'accès physique aux points d'accès, passerelles, dispositifs portables, matériel réseau/communications et lignes de télécommunication sans-fil.</p>	<p>9.1.3 Vérifier que l'accès physique aux points d'accès, passerelles, dispositifs portables, matériel réseau/communications et lignes de télécommunication sans-fil est restreint de la manière appropriée.</p>	<p>Sans mécanismes de sécurité couvrant les composants et les équipements sans-fil, des utilisateurs malveillants pourraient utiliser les équipements sans-fil de l'entreprise, laissés sans surveillance, pour accéder aux ressources du réseau, voire même connecter leurs propres équipements au réseau sans-fil, obtenant ainsi un accès non autorisé. En outre, la sécurisation du réseau et du matériel de communications empêche les individus malveillants d'intercepter le trafic sur le réseau ou de connecter physiquement leurs propres dispositifs aux ressources réseau câblées.</p>
<p>9.2 Développer des procédures pour distinguer facilement le personnel du site des visiteurs, en incluant :</p> <ul style="list-style-type: none"> • L'identification du nouveau personnel sur le site ou des visiteurs (en assignant des badges par exemple) ; • En changeant les conditions d'accès ; • La révocation ou l'élimination de 	<p>9.2.a Examiner les processus documentés pour vérifier que les procédures sont définies pour identifier et pour distinguer le personnel du site et les visiteurs.</p> <ul style="list-style-type: none"> • Vérifier que les procédures comprennent les points suivants : • L'identification du nouveau personnel sur le site ou des visiteurs (en assignant des badges par exemple) ; • Changement des conditions d'accès et • La révocation de l'identification du personnel du site et des visiteurs lorsqu'elle est arrivée à expiration (telle que les badges d'identification). 	<p>Identifier les visiteurs autorisés de manière à les distinguer facilement du personnel du site empêche les visiteurs non autorisés de bénéficier d'un accès à des zones contenant des données de titulaires de carte.</p>

Conditions PCI DSS	Procédures de test	Directive
<p>l'identification du personnel du site et des visiteurs lorsqu'elle est arrivée à expiration (telle que les badges d'identification).</p>	<p>9.2.b Examiner les méthodes d'identification (comme les badges) et observer les processus pour identifier et distinguer le personnel du site et les visiteurs, afin de vérifier que :</p> <ul style="list-style-type: none"> • Les visiteurs sont clairement identifiés et • Il est facile de distinguer le personnel du site des visiteurs. <p>9.2.c Vérifier que l'accès au processus d'identification (tel que le système de badge) est limité au personnel autorisé.</p>	
<p>9.3 Contrôler l'accès physique du personnel du site aux zones sensibles comme suit :</p> <ul style="list-style-type: none"> • L'accès doit être autorisé est basé sur les fonctions professionnelles individuelles. • L'accès est immédiatement révoqué à la cessation de fonction de l'employé et tous les mécanismes d'accès physique, tels que les clés, cartes d'accès, etc., sont rendus ou désactivés. 	<p>9.3.a Pour un échantillon du personnel du site ayant un accès physique aux zones sensibles, interroger le personnel responsable et observer les listes de contrôle d'accès pour vérifier que :</p> <ul style="list-style-type: none"> • L'accès à la zone sensible est autorisé. • L'accès est nécessaire pour les fonctions professionnelles de cette personne. <p>9.3.b Observer l'accès du personnel aux zones sensibles pour vérifier que tout le personnel est autorisé avant d'en obtenir l'accès.</p> <p>9.3.c Sélectionner un échantillon d'employés ayant récemment cessé leurs activités et examiner les listes de contrôle d'accès pour vérifier que ce personnel n'a aucun accès physique aux zones sensibles.</p>	<p>Le contrôle de l'accès physique aux zones sensibles permet d'assurer que seul le personnel autorisé ayant un besoin professionnel légitime peut en obtenir l'accès.</p> <p>Lorsqu'un membre du personnel quitte l'organisation, tous les mécanismes d'accès physiques doivent être rendus ou désactivés rapidement (dès que possible) après son départ pour garantir qu'il ne puisse pas obtenir un accès physique aux zones sensibles après la cessation de ses fonctions.</p>

Conditions PCI DSS	Procédures de test	Directive
<p>9.4 Mettre en œuvre des procédures pour identifier et autoriser les visiteurs.</p> <p>Les procédures doivent inclure les points suivants :</p>	<p>9.4 Vérifier que des autorisations de visiteurs et les contrôles d'accès sont en place comme suit :</p>	<p>Les contrôles de visiteurs sont d'une grande importance pour réduire la capacité des personnes non autorisées ou malveillantes à accéder aux installations (et éventuellement aux données de titulaires de carte).</p>
<p>9.4.1 Les visiteurs sont autorisés avant d'entrer et accompagnés en permanence dans les zones où sont traitées et conservées les données de titulaires de carte.</p>	<p>9.4.1.a Observer les procédures et interroger le personnel pour vérifier que les visiteurs doivent être autorisés avant d'entrer et accompagnés en permanence dans les zones où sont traitées et conservées les données de titulaires de carte.</p> <p>9.4.1.b Observer l'utilisation des badges de visiteur ou des autres formes d'identification afin de vérifier qu'un badge jeton physique ne permet pas d'accéder sans accompagnement aux zones physiques où les données de titulaires de carte sont stockées ou traitées.</p>	<p>Les contrôles de visiteurs assurent que ceux-ci sont identifiables en tant que visiteurs de sorte que le personnel puisse surveiller leurs activités et que leur accès est limité à la durée de leur visite légitime.</p> <p>Assurer que les badges de visiteurs soient retournés après expiration ou une fois la visite terminée empêchera les individus malveillants d'utiliser un passe autorisé précédemment pour obtenir un accès physique au bâtiment une fois que la visite est terminée.</p>
<p>9.4.2 Les visiteurs sont identifiés et un badge ou autre forme d'identification leur est remis avec une date limite d'utilisation, qui distingue clairement les visiteurs du personnel du site.</p>	<p>9.4.2.a Observer les gens au sein de l'établissement afin de vérifier l'utilisation des badges visiteur et pour assurer qu'ils permettent de clairement distinguer les visiteurs du personnel du site.</p> <p>9.4.2.b Vérifier que les badges des visiteurs, ou autres formes d'identification, portent une date d'expiration.</p>	<p>Un registre des visiteurs comportant un minimum d'informations concernant le visiteur est une manière facile et peu onéreuse qui aidera à identifier les accès physiques aux bâtiments ou aux salles et les accès potentiels aux données de titulaires de carte.</p>
<p>9.4.3 Les visiteurs doivent rendre le badge ou autre forme d'identification physique avant de quitter les locaux ou à la date d'expiration.</p>	<p>9.4.3 Observer les visiteurs qui quittent les locaux pour vérifier qu'on leur demande de restituer leur badge ou autre forme d'identification à la sortie ou à l'expiration.</p>	
<p>9.4.4 Un registre des visites est utilisé pour maintenir un suivi d'audit de l'activité des visiteurs aux locaux ainsi qu'aux salles informatiques et aux centres de données où sont stockées ou transmises les données de titulaires de carte.</p> <p>Y consigner le nom du visiteur, l'entreprise qu'il représente et le</p>	<p>9.4.4.a Vérifier qu'un registre des visites est utilisé pour consigner l'accès physique aux locaux ainsi qu'aux salles informatiques et aux centres de données où sont stockées ou transmises les données de titulaires de carte.</p> <p>9.4.4.b Vérifier que ce qui suit est consigné dans le journal :</p> <ul style="list-style-type: none"> • Le nom du visiteur, • La société représentée et • Le personnel du site qui autorise l'accès physique. 	

Conditions PCI DSS	Procédures de test	Directive
<p>personnel du site qui autorise son accès physique.</p> <p>Conserver ce registre pendant trois mois au minimum, sauf stipulation contraire de la loi.</p>	<p>9.4.4.c Vérifier que le journal est conservé pendant au moins trois mois.</p>	
<p>9.5 Assurer la sécurité physique de tous les supports.</p>	<p>9.5 Vérifier que les procédures de protection des données de titulaires de carte comprennent le contrôle de la sécurité physique de tous les supports (entre autres, ordinateurs, supports électroniques amovibles, réseaux, reçus et rapports sur papier, et fax).</p>	<p>Les contrôles de la sécurité physique des supports sont destinés à empêcher les personnes non autorisées d'accéder aux données de carte contenues sur n'importe quel type de support. Les données de titulaires de carte sont susceptibles d'être consultées, copiées ou scannées sans autorisation si elles se trouvent sur un support portable ou amovible, sont imprimées ou sont laissées sur le bureau d'un employé, sans protection.</p>
<p>9.5.1 Ranger les sauvegardes sur support en lieu sûr, de préférence hors des locaux de l'installation, par exemple sur un autre site ou un site de secours, ou encore un site de stockage commercial. Inspecter la sécurité du site au moins une fois par an.</p>	<p>9.5.1 Vérifier que la sécurité du site de stockage est examinée au moins une fois par an pour confirmer que le stockage sur les supports de sauvegarde est sécurisé.</p>	<p>Si elles sont stockées dans un local non sécurisé, les sauvegardes contenant les données de titulaires de carte peuvent être facilement perdues, volées ou copiées à des fins malveillantes.</p> <p>Un examen régulier du site de stockage permet à l'organisation de minimiser les risques de sécurité identifiés avec promptitude et de minimiser les risques potentiels.</p>
<p>9.6 Assurer un contrôle strict de la distribution interne ou externe de tout type de support, notamment ce qui suit :</p>	<p>9.6 Vérifier qu'une politique est en place pour le contrôle de la distribution des supports, et que celle-ci couvre tous les supports distribués, y compris ceux qui sont remis aux individus.</p>	<p>Envisager de mettre en place des procédures et des processus de protection des données de titulaires de carte se trouvant sur les supports distribués à des utilisateurs internes et/ou externes. En l'absence de telles procédures, ces données peuvent être perdues, volées ou utilisées à des fins frauduleuses.</p>

Conditions PCI DSS	Procédures de test	Directive
<p>9.6.1 Classer les supports afin de déterminer la sensibilité des données qu'ils contiennent.</p>	<p>9.6.1 Vérifier que tous les supports sont classés afin de déterminer la sensibilité des données qu'ils contiennent.</p>	<p>Il est important que les supports soient identifiés de manière à ce que ce statut de classification soit facilement identifié. S'ils ne sont pas identifiés comme confidentiels, les supports peuvent ne pas être protégés de la manière appropriée ou être perdus ou volés.</p> <p>Remarque : Cela ne signifie pas que les médias ont besoin d'être ornés d'étiquettes « confidentielles », l'objectif de cette condition est que l'organisation ait des supports identifiés contenant les données sensibles afin qu'elle puisse les protéger.</p>
<p>9.6.2 Envoyer les supports par coursier sécurisé ou toute autre méthode d'expédition qui peut faire l'objet d'un suivi précis.</p>	<p>9.6.2.a Interroger le personnel et examiner les archives pour vérifier que tous les supports expédiés à l'extérieur des locaux sont consignés et autorisés par les responsables, et qu'ils sont envoyés par coursier sécurisé ou toute autre méthode d'expédition qui peut faire l'objet d'un suivi.</p> <p>9.6.2.b Choisir un échantillon récent de registres couvrant plusieurs jours de suivi hors site de tous les supports, et vérifier que les informations de suivi sont consignées.</p>	<p>S'ils sont envoyés sans suivi, par exemple par courrier postal normal, les supports risquent d'être perdus ou volés. L'utilisation des services d'un coursier sécurisé pour l'envoi de tout support contenant des données de titulaires de carte permet à l'organisation d'utiliser son système de suivi afin d'inventorier et localiser chaque envoi.</p>
<p>9.6.3 Assurer que les responsables approuvent le déplacement de tout support déplacé d'une zone sécurisée (en particulier s'ils sont distribués à des individus).</p>	<p>9.6.3 Sélectionner un échantillon récent de registres couvrant plusieurs jours de suivi hors site de tous les supports. En examinant les registres et en interrogeant le personnel responsable, vérifier que l'autorisation correcte des responsables est obtenue pour le déplacement de tout support déplacé d'une zone sécurisée (y compris lorsque les supports sont distribués à des individus).</p>	<p>Sans un processus ferme pour garantir que tous les mouvements de support sont approuvés avant que le support ne soit enlevé de zones sécurisées, le support ne sera pas suivi ou protégé correctement et son emplacement sera inconnu, ce qui pourrait mener à des supports perdus ou volés.</p>
<p>9.7 Assurer un contrôle strict du stockage et de l'accessibilité des supports.</p> <p>9.7.1 Tenir de manière appropriée les journaux d'inventaire de tous les supports et effectuer un inventaire des supports au moins une fois par an.</p>	<p>9.7 Obtenir et examiner la politique de contrôle du stockage et de la gestion des supports, et vérifier qu'elle stipule l'inventaire des supports à intervalles réguliers.</p> <p>9.7.1 Examiner les journaux d'inventaire des supports pour vérifier qu'ils sont maintenus et que les inventaires de support sont réalisés au moins une fois par an.</p>	<p>Sans des méthodes d'inventaire et de contrôles du stockage méticuleux, le vol ou l'absence de supports pourraient passer inaperçus pendant une période indéterminée.</p> <p>Si les supports ne font pas l'objet d'un inventaire, leur vol ou leur absence pourraient passer inaperçus pendant une période indéterminée ou même jamais.</p>

Conditions PCI DSS	Procédures de test	Directive
<p>9.8 Détruire les supports lorsqu'ils ne sont plus nécessaires à des fins professionnelles ou légales comme suit :</p>	<p>9.8 Examiner la politique de destruction périodique des supports et vérifier qu'elle couvre tous les supports et définit des conditions pour les points suivants :</p> <ul style="list-style-type: none"> • Les documents papier doivent être déchiquetés, brûlés ou réduits en pâte de manière à avoir l'assurance raisonnable qu'ils ne pourront pas être constitués. • Les conteneurs de stockage utilisés pour les documents qui sont détruits doivent être sécurisés. • Les données de titulaires de carte sur support électronique doivent être rendues irrécupérables (par exemple, à l'aide d'un programme de nettoyage sécurisé conformément aux normes du secteur en matière d'élimination sécurisée ou par destruction physique du média). 	<p>Si les mesures nécessaires ne sont pas prises pour détruire les informations contenues sur les supports, disques durs, lecteurs portables, CD ou DVD ou papier, avant leur élimination, des individus malveillants peuvent être en mesure de récupérer des informations sur les supports éliminés et la sécurité des données s'en trouverait compromise. Par exemple, des individus malveillants peuvent utiliser une technique dénommée le « dumpster diving », qui consiste à fouiller les poubelles et les corbeilles, afin d'y rechercher des informations utiles pour lancer une attaque.</p>
<p>9.8.1 Déchiqueter, brûler ou réduire en pâte les documents papier de sorte que les données de titulaires de carte ne puissent pas être reconstituées. Sécuriser les conteneurs de stockage utilisés pour les documents qui doivent être détruits.</p>	<p>9.8.1.a Interroger le personnel et examiner les procédures pour vérifier que les documents papier sont déchiquetés, brûlés ou réduits en pâte de manière à avoir l'assurance raisonnable qu'ils ne pourront pas être reconstitués.</p> <p>9.8.1.b Examiner les conteneurs dans lesquels sont stockées les documents à détruire afin de vérifier qu'ils sont sécurisés.</p>	<p>Les containers de stockage sécurisés utilisés pour le stockage des documents qui vont être détruits empêchent que les informations sensibles ne soient capturées lorsque les documents sont récoltés. Par exemple, les containers de documents « à déchiqueter » doivent être munis de cadenas pour empêcher l'accès à leur contenu ou un alliage physique prévient l'accès à l'intérieur du container.</p>
<p>9.8.2 Rendre les données de titulaires de carte sur support électronique irrécupérables de sorte que les informations ne puissent pas être reconstituées.</p>	<p>9.8.2 Vérifier que les données de titulaires de carte sur support électronique sont rendues irrécupérables (par exemple, à l'aide d'un programme de nettoyage sécurisé conformément aux normes du secteur en matière d'élimination sécurisée, ou par destruction physique du média).</p>	<p>L'effacement, la démagnétisation ou la destruction physique (comme le broyage ou l'effacement définitif du disque dur) sont des exemples de méthodes permettant la destruction sécurisée de supports électroniques.</p>

Conditions PCI DSS	Procédures de test	Directive
<p>9.9 Protéger les dispositifs qui capturent les données de carte de paiement par interaction physique directe avec la carte des manipulations malveillantes et des substitutions.</p> <p><i>Remarque : Ces conditions s'appliquent aux dispositifs de lecture de carte utilisés dans les transactions pour lesquelles la carte est présente (c'est-à-dire, une lecture de piste ou de puce) au point de vente. Cette condition n'est pas destinée à être appliquée pour les composants d'entrée manuelle à touches tels que les claviers d'ordinateur et les claviers de POS.</i></p>	<p>9.9 Examiner les politiques et les procédures documentées pour vérifier que les points suivants sont inclus :</p> <ul style="list-style-type: none"> • Maintenir une liste des appareils ; • Inspecter régulièrement les appareils pour s'assurer qu'ils n'ont pas été manipulés ou substitués ; • Former le personnel pour qu'il soit conscient des comportements suspects et pour signaler les manipulations ou la substitution des appareils. 	<p>Les personnes malveillantes essaient de voler les données de titulaires de carte en volant et/ou en manipulant les appareils de lecture de carte et les terminaux. Par exemple, ils essayeront de voler les appareils afin de pouvoir apprendre comment y pénétrer et ils essayeront souvent de remplacer les appareils légitimes par des appareils frauduleux qui leur envoient les informations de carte de paiement dès que la carte est entrée dans l'appareil. Les personnes malveillantes essayeront également « d'écrémer » les composants à l'extérieur de l'appareil qui sont conçus pour capturer les détails de carte de paiement avant même qu'ils n'entrent dans l'appareil, par exemple, en ajoutant un lecteur de carte supplémentaire pour que les détails de carte de paiement soient capturés deux fois, une fois par le composant d'une personne malveillante et une fois par le composant légitime de l'appareil. De cette manière, les transactions peuvent tout de même avoir lieu sans interruption lorsque la personne malveillante « écrème » les informations de carte de paiement pendant le procédé.</p> <p>Cette condition est recommandée, mais elle n'est pas requise pour les composants d'entrée manuelle à touches tels que les claviers d'ordinateur et les claviers de POS.</p> <p>Les meilleures pratiques supplémentaires pour la prévention de l'écrémage sont disponibles sur le site Web du PCI SSC.</p>
<p>9.9.1 Maintenir une liste d'appareils à jour. La liste doit inclure les points suivants :</p> <ul style="list-style-type: none"> • Marque et modèle de l'appareil ; • L'emplacement de l'appareil (par exemple, l'adresse du site ou de l'installation où se trouve 	<p>9.9.1.a Examiner la liste des appareils pour vérifier qu'elle comprend les éléments suivants :</p> <ul style="list-style-type: none"> • Marque et modèle de l'appareil ; • L'emplacement de l'appareil (par exemple, l'adresse du site ou de l'installation où se trouve l'appareil) ; • Le numéro de série de l'appareil ou autre méthode d'identification unique. 	<p>Conserver une liste des appareils à jour aide une organisation à suivre les emplacements où les appareils sont censés être et à identifier rapidement les appareils manquants ou perdus.</p> <p>La méthode de maintenance d'une liste des appareils peut être automatisée (par exemple, à l'aide d'un système de gestion des appareils) ou</p>

Conditions PCI DSS	Procédures de test	Directive
l'appareil) ; <ul style="list-style-type: none"> Le numéro de série de l'appareil ou autre méthode d'identification unique. 	<p>9.9.1.b Sélectionner un échantillon d'appareils dans la liste et observer leurs emplacements pour vérifier que la liste est précise et tenue à jour.</p> <p>9.9.1.c Interroger le personnel pour vérifier que la liste des appareils est maintenue à jour lorsque des appareils sont ajoutés, déplacés, retirés du service, etc.</p>	manuelle (par exemple, documentée sur support électronique ou papier). Pour les appareils sur la route, l'emplacement peut inclure le nom de l'employé auquel l'appareil est affecté.
<p>9.9.2 Inspecter régulièrement la surface des appareils pour voir si elle présente des signes de manipulations malveillantes (par exemple, l'ajout de</p>	<p>9.9.2.a Examiner les procédures documentées pour vérifier que des processus sont définis pour inclure les points suivants :</p> <ul style="list-style-type: none"> Procédures d'inspection des appareils ; Fréquence des inspections. 	Les inspections régulières aideront les organisations à détecter plus rapidement les manipulations malveillantes ou le remplacement d'un appareil, et donc de minimiser l'impact

Conditions PCI DSS	Procédures de test	Directive
<p>copieur de carte sur l'appareil), ou de substitution (par exemple, en inspectant le numéro de série ou autre caractéristique de l'appareil pour vérifier qu'il n'a pas été substitué par un appareil frauduleux).</p> <p>Remarque : Les exemples de signes qu'un appareil aurait pu être la victime de manipulations malveillantes ou substituées comprennent les fixations de câble ou de dispositifs inattendus à l'appareil, les étiquettes de sécurité manquantes ou modifiées, un boîtier cassé ou de couleur différente, ou un changement du numéro de série ou autres marques externes.</p>	<p>9.9.2.b Interroger le personnel responsable et examiner les processus d'inspection pour vérifier que :</p> <ul style="list-style-type: none"> • Le personnel est conscient des procédures d'inspection des appareils. • Tous les appareils sont inspectés régulièrement pour découvrir les évidences de manipulation malveillantes ou de substitutions. 	<p>potentiel de l'utilisation d'appareils frauduleux.</p> <p>Le type d'inspection dépendra de l'appareil, par exemple, les photographies d'appareil dont on sait qu'ils sont sécurisés peuvent être utilisées pour comparer l'aspect actuel de l'appareil à son aspect d'origine afin de voir s'il a changé. Une autre option pourrait être d'utiliser un marqueur, tel qu'une marque UV léger, pour marquer les surfaces des appareils et les orifices de l'appareil afin que toute manipulation malveillante ou tout remplacement soit apparent. Souvent, les personnes malveillantes remplaceront le boîtier extérieur d'un appareil pour dissimuler leurs manipulations malveillantes et ces méthodes peuvent aider à détecter ce type d'activité. Les fournisseurs d'appareil doivent également être capables de donner des consignes de sécurité et des guides de « comment faire » pour aider à déterminer si l'appareil a été victime de manipulations malveillantes.</p> <p>La fréquence des inspections dépendra des facteurs tels que l'emplacement de l'appareil et si l'appareil est ou non sous surveillance. Par exemple, les appareils laissés sans supervision dans les zones publiques par le personnel de l'organisation ont plus de chances de subir des inspections fréquentes que les appareils qui sont conservés dans des zones sécurisées ou qui sont supervisés lorsqu'ils sont accessibles au public. Le type et la fréquence des inspections sont déterminés par le type de commerçant, ainsi que le définit le processus annuel d'évaluation des risques.</p>

Conditions PCI DSS	Procédures de test	Directive
<p>9.9.3 Assurer la formation du personnel afin qu'il soit conscient des tentatives de manipulation malveillantes ou de remplacement des appareils. La formation doit inclure les points suivants :</p> <ul style="list-style-type: none"> • Vérifier l'identité de tout tiers prétendant faire partie du personnel de maintenance ou de réparation, avant de lui accorder l'accès pour modifier ou dépanner les appareils. • Ne pas installer, remplacer ou renvoyer pas l'appareil sans vérification. • Être conscient des comportements suspects autour des appareils (par exemple, les tentatives de débrancher ou d'ouvrir les appareils par des personnes inconnues). • Signaler les comportements suspects et les indications de manipulation malveillante ou de substitution de l'appareil au personnel approprié (par exemple, à un responsable ou à un agent de la sécurité). 	<p>9.9.3.a Examiner les documents de formation pour le personnel au point de vente pour vérifier qu'ils comprennent la formation à ce qui suit :</p> <ul style="list-style-type: none"> • La vérification de l'identité de tout tiers prétendant faire partie du personnel de maintenance ou de réparation, avant de lui accorder l'accès pour modifier ou dépanner les appareils. • Ne pas installer, remplacer ou renvoyer pas l'appareil sans vérification. • Être conscient des comportements suspects autour des appareils (par exemple, les tentatives de débrancher ou d'ouvrir les appareils par des personnes inconnues). • Signaler les comportements suspects et les indications de manipulation malveillante ou de substitution de l'appareil au personnel approprié (par exemple, à un responsable ou à un agent de la sécurité). <p>9.9.3.b Interroger un échantillon du personnel au point de vente pour vérifier qu'il a reçu la formation adéquate et qu'il connaît les procédures pour ce qui suit :</p> <ul style="list-style-type: none"> • La vérification de l'identité de tout tiers prétendant faire partie du personnel de maintenance ou de réparation, avant de lui accorder l'accès pour modifier ou dépanner les appareils. • Ne pas installer, remplacer ou renvoyer pas l'appareil sans vérification. • Être conscient des comportements suspects autour des appareils (par exemple, les tentatives de débrancher ou d'ouvrir les appareils par des personnes inconnues). • Signaler les comportements suspects et les indications de manipulation malveillante ou de substitution de l'appareil au personnel approprié (par exemple, à un responsable ou à un agent de la sécurité). 	<p>Souvent les personnes malveillantes prétendent être des agents de maintenance afin d'accéder aux appareils de POS. Tous les tiers demandant à avoir accès à l'appareil doivent toujours être vérifiés avant d'obtenir cet accès, par exemple, en vérifiant avec la direction, ou en contactant la société chargée de la maintenance (telle que le fournisseur ou l'acquéreur) au POS à fin de vérification. De nombreuses personnes malveillantes essayeront de tromper le personnel en s'habillant pour l'occasion (par exemple, en transportant des caisses à outil et en portant des vêtements de travail) et il est également possible qu'ils connaissent l'emplacement des appareils, il est donc important que le personnel soit formé pour qu'il suive en tout temps les procédures.</p> <p>Une autre technique utilisée par les personnes malveillantes consiste à substituer un « nouveau » système de point de vente avec des instructions pour la substitution dans un système légitime et de « renvoyer » le système légitime à une adresse spécifiée. Les personnes malveillantes peuvent même fournir une enveloppe de retour de courrier, dans la mesure où ils sont fort désireux d'obtenir ces appareils. Le personnel vérifie toujours avec son responsable ou son fournisseur que l'appareil est légitime et qu'il provient d'une source approuvée avant de l'installer ou de l'utiliser dans l'entreprise.</p>

Conditions PCI DSS	Procédures de test	Directive
<p>9.10 Assurer que les politiques de sécurité et les procédures opérationnelles pour la restriction de l'accès aux données de titulaires de carte sont documentées, utilisées et connues de toutes les parties concernées.</p>	<p>9.10 Examiner la documentation et interroger le personnel pour vérifier que les politiques de sécurité et les procédures opérationnelles pour la restriction de l'accès physique aux données de titulaires de carte sont :</p> <ul style="list-style-type: none"> • Documentées • Utilisées et • Connues de toutes les parties concernées. 	<p>Le personnel doit être conscient et suivre les politiques de sécurité et les procédures opérationnelles pour restreindre l'accès physique aux données de titulaires de carte et aux systèmes CDE sur une base continue.</p>

Surveillance et test réguliers des réseaux

Condition 10 : Effectuer le suivi et surveiller tous les accès aux ressources réseau et aux données de titulaires de carte

Les mécanismes de journalisation et la possibilité de suivre les activités des utilisateurs sont essentiels pour prévenir, détecter ou minimiser l'impact d'une altération des données. La présence de journaux dans tous les environnements permet de suivre de près, d'émettre des alertes et d'analyser les incidents éventuels. En l'absence de journaux retraçant les activités du système, il est très difficile, sinon impossible, de déterminer la cause d'une anomalie.

Conditions PCI DSS	Procédures de test	Directive
10.1 Implémenter des cheminements d'audit pour relier tous les accès aux composants de système à chaque utilisateur individuel.	10.1 Vérifier, par l'observation et en interrogeant l'administrateur du système, que : <ul style="list-style-type: none"> • Les cheminements d'audit sont activés et actifs pour les composants de système. • L'accès aux composants de système est relié aux utilisateurs individuels. 	Il est essentiel de disposer d'un processus ou d'un système qui établisse le lien entre l'accès d'un utilisateur et les composants de système auxquels il a accédé. Ce système génère des registres d'audit et permet de retracer les activités suspectes jusqu'à un utilisateur particulier.
10.2 Mettre en œuvre des vérifications à rebours automatisées pour tous les composants de système afin de reconstituer les événements suivants :	10.2 En interrogeant le personnel responsable, en observant les journaux d'audit et les paramètres de ces journaux d'audit, prendre les mesures décrites ci-après :	La vérification à rebours des activités suspectes alerte l'administrateur système, envoie les données à d'autres mécanismes de surveillance (comme des systèmes de détection d'intrusion) et établit un historique pour le suivi après incident. Consigner les événements suivants permet à l'organisation d'identifier et de retracer des activités potentiellement malveillantes.
10.2.1 Tous les accès des utilisateurs individuels aux données de titulaires de carte	10.2.1 Vérifier que tous les accès des utilisateurs aux données de titulaires de carte sont consignés.	Les individus malveillants peuvent avoir connaissance d'un compte utilisateur et obtenir l'accès aux systèmes de l'environnement des données de titulaires de carte ou créer un nouveau compte, non autorisé, afin d'accéder à ces données. Enregistrer tous les accès individuels aux données de titulaires de carte permet d'identifier les comptes compromis ou utilisés de manière illicite.

Conditions PCI DSS	Procédures de test	Directive
<p>10.2.2 Toutes les actions exécutées par tout utilisateur avec des droits racine ou administrateur</p>	<p>10.2.2 Vérifier que toutes les actions exécutées par tout utilisateur avec des droits racine ou administrateur sont consignées.</p>	<p>Les comptes possédant des privilèges accrus, comme les comptes « administrateur » ou « racine », sont potentiellement plus dangereux pour la sécurité ou la fonctionnalité opérationnelle d'un système s'ils venaient à être compromis. Sans un journal des activités exécutées, une organisation est incapable de retracer tout problème provoqué par une erreur administrative ou d'une utilisation illicite d'un privilège à l'action et à l'individu spécifiques.</p>
<p>10.2.3 Accès à toutes les vérifications à rebours</p>	<p>10.2.3 Vérifier que les accès à toutes les vérifications à rebours sont consignés.</p>	<p>Des utilisateurs malveillants tentent souvent de modifier les journaux d'audit afin de dissimuler leurs activités et un enregistrement des accès permet à une organisation de retracer toutes les incohérences ou altérations potentielles des journaux pour un compte individuel. Avoir accès aux journaux identifiant les changements, les additions et les suppressions pourrait aider à retracer les étapes suivies par le personnel non autorisé.</p>
<p>10.2.4 Tentatives d'accès logique non valides</p>	<p>10.2.4 Vérifier que les tentatives d'accès logique non valides sont consignées.</p>	<p>Les individus malveillants font souvent plusieurs tentatives pour accéder aux systèmes ciblés. De multiples tentatives infructueuses de connexion peuvent indiquer qu'un utilisateur non autorisé tente d'utiliser la « force brute » ou de deviner un mot de passe.</p>
<p>10.2.5 L'utilisation et les modifications des mécanismes d'identification et d'authentification, y compris, mais sans s'y limiter, la création de nouveaux comptes et l'élévation de privilèges, et toutes les modifications, additions ou suppressions aux comptes avec des privilèges racines ou administratifs</p>	<p>10.2.5.a Vérifier que l'utilisation des mécanismes d'identification et d'authentification est consignée.</p>	<p>Sans savoir qui était connecté au moment d'un incident, il est impossible d'identifier les comptes qui ont pu être utilisés. En outre, les utilisateurs malveillants peuvent tenter de manipuler les contrôles d'authentification avec l'intention de les contourner ou d'usurper un compte valide.</p>
	<p>10.2.5.b Vérifier que toutes les élévations de privilège sont consignées.</p>	
	<p>10.2.5.c Vérifier que tous les changements, additions ou suppressions apportés à un compte avec privilèges racine ou administratives sont consignées.</p>	

Conditions PCI DSS	Procédures de test	Directive
10.2.6 Initialisation, interruption ou pause des journaux d'audit	10.2.6 Vérifier que ce qui suit est consigné dans le journal : <ul style="list-style-type: none"> • L'initialisation des journaux d'audit ; • L'Interruption ou pause des journaux d'audit. 	La désactivation (ou pause) des journaux d'audit avant de se livrer à des activités illicites est une pratique courante des individus mal intentionnés souhaitant éviter d'être détectés. L'initialisation des journaux d'audit peut indiquer que la fonction de journalisation a été désactivée par un utilisateur pour dissimuler son activité.
10.2.7 Création et suppression d'objets au niveau système	10.2.7 Vérifier que la création et la suppression d'objets au niveau du système sont consignées.	Souvent, un logiciel malveillant crée ou remplace des objets au niveau système, sur le système visé, afin de prendre le contrôle d'une fonction particulière ou de l'activité de ce système. En effectuant les enregistrements dans le journal lorsque les objets au niveau du système, tels que les tableaux de base de données ou les procédures enregistrées, sont créés ou supprimés, il sera plus facile de déterminer si ces modifications ont été autorisées.
10.3 Consigner dans les vérifications à rebours au moins les entrées suivantes pour chaque événement :	10.3 En interrogeant le personnel et en observant les journaux d'audit pour chaque événement vérifiable (à partir du point 10.2), et accomplissez ce qui suit :	Enregistrer ces détails pour les événements vérifiables au point 10.2 permet d'identifier rapidement une intrusion éventuelle, avec suffisamment de détails pour connaître l'auteur, l'objet, l'emplacement, le moment et la méthode employée.
10.3.1 Identification de l'utilisateur	10.3.1 Vérifier que l'identification d'utilisateur est incluse dans les entrées des journaux.	
10.3.2 Type d'événement	10.3.2 Vérifier que le type d'événement est inclus dans les entrées des journaux.	
10.3.3 Date et heure	10.3.3 Vérifier que l'horodatage est inclus dans les entrées de journaux.	
10.3.4 Indication de succès ou d'échec	10.3.4 Vérifier que l'indication de succès ou d'échec est incluse dans les entrées de journaux.	
10.3.5 Origine de l'événement	10.3.5 Vérifier que l'origine de l'événement est incluse dans les entrées de journaux.	
10.3.6 Identité ou nom des données, du composant du système ou de la ressource affectés	10.3.6 Vérifier que l'identité ou le nom des données, du composant du système ou de la ressource affectés est inclus dans les entrées de journaux.	

Conditions PCI DSS	Procédures de test	Directive
<p>10.4 À l'aide d'une technologie de synchronisation temporelle, synchroniser tous les systèmes d'horloge et temporels critiques et s'assurer que les éléments suivants sont mis en œuvre pour l'acquisition, la distribution et l'enregistrement du temps.</p> <p>Remarque : Le protocole Network Time Protocol (NTP -Protocole d'Heure Réseau) est un exemple de technologie de synchronisation temporelle.</p>	<p>10.4 Examiner les normes et les processus de configuration pour vérifier que la technologie de synchronisation de temporelle est mise en œuvre et conservée à jour selon les conditions 6.1 et 6.2 de la norme PCI DSS.</p>	<p>La technologie de synchronisation temporelle permet de synchroniser les horloges de systèmes multiples. Lorsque les horloges ne sont pas correctement synchronisées, il peut être difficile voire impossible, de comparer les fichiers journaux de systèmes différents et l'établissement de la séquence exacte d'un événement (un point crucial pour les analyses légales en cas de violation du système). Pour les équipes légales enquêtant après un incident, la précision et l'uniformité de l'heure sur l'ensemble des systèmes et celle de chaque activité sont essentielles pour déterminer la manière dont les systèmes ont été compromis.</p>
<p>10.4.1 L'heure des systèmes critiques est correcte et la même pour tous.</p>	<p>10.4.1.a Examiner le processus d'acquisition et de distribution et de stockage de l'heure juste dans l'organisation pour vérifier que :</p> <ul style="list-style-type: none"> • Seuls le ou les serveurs d'heure centrale désignée reçoivent des signaux de sources externes et que ces derniers se basent sur le temps atomique universel ou l'UTC (temps universel coordonné). • Lorsqu'il y a plus d'un serveur d'heure désigné, les serveurs d'heure se basent l'un sur l'autre pour conserver une heure précise. • Les systèmes reçoivent les informations concernant l'heure uniquement à partir des serveurs d'heure centrale désignés. <p>10.4.1.b Observer les réglages de paramètre de système liés à l'heure sur un échantillon de composants de système pour vérifier :</p> <ul style="list-style-type: none"> • Seuls le ou les serveurs d'heure centrale désignée reçoivent des signaux de sources externes et que ces derniers se basent sur le temps atomique universel ou l'UTC (temps universel coordonné). • Lorsqu'il y a plus d'un serveur d'heure désigné, le ou les serveurs d'heure centrale se basent l'un sur l'autre pour conserver une heure précise. • Les systèmes reçoivent l'heure uniquement à partir des serveurs d'heure centrale désignés. 	

Conditions PCI DSS	Procédures de test	Directive
<p>10.4.2 Les données temporelles sont protégées.</p>	<p>10.4.2.a Examiner les configurations du système et des paramètres de synchronisation temporelle pour vérifier que l'accès aux données temporelles est restreint au seul personnel dont l'accès à ces données est justifié par un besoin professionnel.</p> <p>10.4.2.b Examiner les configurations du système, les paramètres, journaux et processus de synchronisation temporelle afin de vérifier que tout changement aux paramètres temporels sur des systèmes critiques est consigné, surveillé et vérifié.</p>	
<p>10.4.3 Les paramètres temporels sont reçus de sources temporelles reconnues par le secteur.</p>	<p>10.4.3 Examiner les configurations des systèmes pour vérifier que les serveurs temporels acceptent des mises à jour temporelles de sources externes spécifiques, reconnues par le secteur (afin de prévenir toute tentative malveillante de changer l'horloge). Il est également possible de crypter ces mises à jour avec une clé symétrique, et de créer des listes de contrôle d'accès qui indiquent les adresses IP des machines clientes qui recevront les mises à jour temporelles (afin d'empêcher toute utilisation non autorisée des serveurs d'horloge internes).</p>	
<p>10.5 Protéger les vérifications à rebours de sorte qu'elles ne puissent pas être modifiées.</p>	<p>10.5 Interroger les administrateurs de système et examiner les autorisations et configurations de système pour vérifier que les cheminements d'audit sont sécurisés pour qu'ils ne puissent pas être modifiés comme suit :</p>	<p>Un individu malveillant, ayant pénétré sur le réseau, tentera souvent de modifier les journaux d'audit afin de dissimuler ses activités. Sans une protection adéquate des journaux d'audit, il ne sera pas possible d'en garantir l'intégralité, l'exactitude et l'intégrité et ils seront inutiles en tant qu'outil d'investigation une fois le système compromis.</p>
<p>10.5.1 Limiter l'affichage des vérifications à rebours aux utilisateurs qui en ont besoin pour mener à bien leur travail.</p>	<p>10.5.1 Seul un individu qui en a un besoin professionnel réel peut consulter les fichiers de journaux de vérification.</p>	<p>Une protection adéquate des journaux d'audit comprend un contrôle d'accès robuste (accès limité aux journaux en fonction du « besoin d'en connaître ») et l'utilisation d'un mécanisme d'isolation interne pour qu'il soit plus difficile de trouver et modifier les journaux.</p>
<p>10.5.2 Protéger les fichiers de vérifications à rebours contre toute modification non autorisée.</p>	<p>10.5.2 Les fichiers de piste d'audits sont protégés contre toute modification non autorisée par des mécanismes de contrôle d'accès, leur isolation physique et/ou l'isolation du réseau.</p>	<p>Sauvegarder rapidement les fichiers journaux sur</p>

Conditions PCI DSS	Procédures de test	Directive
<p>10.5.3 Sauvegarder rapidement les fichiers de vérifications à rebours sur un serveur centralisé réservé à la journalisation ou sur des supports difficiles à altérer.</p>	<p>10.5.3 Les fichiers de piste d'audit sont rapidement sauvegardés sur un serveur centralisé réservé à la journalisation ou sur des supports difficiles à altérer.</p>	<p>un serveur ou un support centralisé difficile à altérer conserve les journaux protégés même si le système qui génère les journaux est compromis.</p>
<p>10.5.4 Inscrire les journaux pour les technologies orientées vers l'extérieur sur un serveur de journal interne centralisé et sécurisé, ou sur un dispositif de support.</p>	<p>10.5.4 Les registres des technologies orientées vers l'extérieur (par exemple, sans-fil, pare-feu, DNS, messagerie) sont écrits sur un serveur de journal interne centralisé et sécurisé ou un support.</p>	<p>Renseigner les journaux depuis des technologies orientées vers l'extérieur, comme le sans-fil, le pare-feu, les serveurs DNS et les serveurs de messagerie, réduit les risques de perte ou de modification de ces journaux, car ils sont mieux protégés au sein du réseau interne.</p> <p>Les journaux peuvent être écrits directement, issus ou copiés des systèmes externes, sur le système ou support interne sécurisé.</p>
<p>10.5.5 Analyser les journaux à l'aide d'un logiciel de surveillance de l'intégrité des fichiers ou de détection des modifications pour s'assurer que les données contenues dans les journaux ne peuvent pas être modifiées sans entraîner le déclenchement d'une alerte (alors que l'ajout de nouvelles données ne doit pas entraîner d'alerte).</p>	<p>10.5.5 Examiner les paramètres de système, les fichiers surveillés et les résultats des activités de surveillance pour vérifier l'utilisation de la surveillance d'intégrité des fichiers ou de logiciel de détection de changement sur les journaux.</p>	<p>La surveillance d'intégrité des fichiers ou les systèmes de détection des changements inspectent les modifications apportées aux fichiers critiques et signalent les modifications. Pour surveiller l'intégrité des fichiers, une entreprise vérifie généralement les fichiers qui ne sont pas régulièrement modifiés, mais dont la modification indique une intrusion possible.</p>
<p>10.6 Examiner les journaux et les événements de sécurité de tous les composants de système pour identifier les anomalies ou les activités suspectes.</p> <p><i>Remarque : Des outils de journalisation, d'analyse et d'alerte peuvent être utilisés pour respecter cette condition.</i></p>	<p>10.6 Effectuer les tâches suivantes :</p>	<p>De nombreuses violations se produisent des jours ou des mois avant d'être détectées. Les examens réguliers des journaux par le personnel ou automatiquement peuvent identifier et résoudre de manière proactive les accès non autorisés à l'environnement de données de titulaires de carte.</p> <p>Le processus d'examen des journaux ne doit pas forcément être manuel. L'utilisation d'outils de journalisation, d'analyse et d'alerte peut aider à faciliter le processus en identifiant les événements du journal qui doivent être examinés.</p>

Conditions PCI DSS	Procédures de test	Directive
<p>10.6.1 Examiner les points suivants au moins une fois par jour :</p> <ul style="list-style-type: none"> • Tous les événements de sécurité • Les journaux de tous les composants de système qui stockent, traitent ou transmettent des CHD et/ou SAD • Les journaux de tous les composants critiques du système • Les journaux de tous les composants de système et de serveur qui remplissent des fonctions de sécurité (par exemple, les pare-feu, les systèmes de détection d'intrusion/systèmes de prévention d'intrusion (IDS/IPS), les serveurs d'authentification, les serveurs de redirection de commerce électronique, etc.) 	<p>10.6.1.a Examiner les politiques et les procédures de sécurité pour vérifier que des procédures sont définies pour l'examen des points suivants au moins une fois par jour, manuellement ou à l'aide d'outils de journalisation :</p> <ul style="list-style-type: none"> • Tous les événements de sécurité • Les journaux de tous les composants de système qui stockent, traitent ou transmettent des CHD et/ou SAD • Les journaux de tous les composants critiques du système • Les journaux de tous les composants de système et de serveur qui remplissent des fonctions de sécurité (par exemple, les pare-feu, les systèmes de détection d'intrusion/systèmes de prévention d'intrusion (IDS/IPS), les serveurs d'authentification, les serveurs de redirection de commerce électronique, etc.) <p>10.6.1.b Observer les processus et interroger le personnel pour vérifier que des procédures suivantes sont mises en œuvre :</p> <ul style="list-style-type: none"> • Tous les événements de sécurité • Les journaux de tous les composants de système qui stockent, traitent ou transmettent des CHD et/ou SAD • Les journaux de tous les composants critiques du système • Les journaux de tous les composants de système et de serveur qui remplissent des fonctions de sécurité (par exemple, les pare-feu, les systèmes de détection d'intrusion/systèmes de prévention d'intrusion (IDS/IPS), les serveurs d'authentification, les serveurs de redirection de commerce électronique, etc.) 	<p>La vérification quotidienne des journaux réduit la durée et l'exposition à une violation potentielle.</p> <p>Des examens quotidiens des événements de sécurité, par exemple, les notifications ou les alertes en cas d'identification d'activités suspectes ou anormales, ainsi que des journaux de composants critiques du système et des journaux de systèmes qui remplissent des fonctions de sécurité, tels que les pare-feu, IDS/IPS, systèmes de surveillance d'intégrité de fichier (FIM), etc. sont nécessaires pour identifier les problèmes potentiels. Remarque que la détermination d'un « événement de sécurité » variera pour chaque organisation et peut inclure une prise en compte du type de technologie, de l'emplacement et des fonctions de l'appareil. Les organisations peuvent aussi souhaiter maintenir une ligne de base de trafic « normal » pour aider à identifier les comportements anormaux.</p>
<p>10.6.2 Examiner régulièrement les journaux de tous les autres composants de système conformément aux politiques et à la stratégie de gestion des risques de l'organisation, ainsi que le détermine l'évaluation de risque annuelle de l'organisation.</p>	<p>10.6.2.a Examiner les politiques et les procédures de sécurité pour vérifier que des procédures sont définies pour l'examen régulier des journaux de tous les autres composants de système, manuellement ou à l'aide d'outils de journalisation, conformément aux politiques et à la stratégie de gestion des risques de l'organisation.</p> <p>10.6.2.b Examiner la documentation d'évaluation des risques de l'entreprise et interroger le personnel pour vérifier que les examens sont effectués conformément aux politiques et à la stratégie de gestion des risques de l'organisation.</p>	<p>Les journaux de tous les autres composants de système doivent également être examinés régulièrement pour identifier les indications de problèmes potentiels ou de tentatives d'accès aux systèmes sensibles par le biais de systèmes moins sensibles. La fréquence des examens doit être déterminée par une évaluation annuelle des risques effectuée par l'organisation.</p>

Conditions PCI DSS	Procédures de test	Directive
<p>10.6.3 Suivi des exceptions et des anomalies identifiées pendant le processus d'examen.</p>	<p>10.6.3.a Examiner les politiques et les procédures de sécurité pour vérifier que des procédures sont définies pour le suivi des exceptions et des anomalies identifiées pendant le processus d'examen.</p> <p>10.6.3.b Observer les processus et interroger le personnel pour vérifier que le suivi des exceptions et des anomalies est effectué.</p>	<p>Si les exceptions et les anomalies identifiées pendant le processus d'examen de journal ne donnent pas lieu à une enquête, l'organisation serait susceptible d'ignorer les activités non autorisées et potentiellement malveillantes qui se produisent sur son propre réseau.</p>
<p>10.7 Conserver l'historique des audits pendant une année au moins, en gardant immédiatement à disposition les journaux des trois derniers mois au moins, à fin d'analyse (par exemple, disponibles en ligne, dans des archives ou pouvant être restaurés à partir d'une sauvegarde).</p>	<p>10.7.a Examiner les politiques et les procédures pour vérifier qu'elles définissent les points suivants :</p> <ul style="list-style-type: none"> • Politiques de conservation des journaux d'audit • Procédures de conservation des journaux d'audit pendant une année au moins, en gardant les journaux des trois derniers mois disponibles immédiatement en ligne. <p>10.7.b Interroger le personnel et examiner les journaux d'audit pour vérifier qu'ils sont disponibles pendant au moins un an.</p> <p>10.7.c Interroger le personnel et observer les processus pour vérifier que les journaux des trois derniers mois au moins sont immédiatement disponibles à des fins d'analyse.</p>	<p>Les journaux doivent être conservés pendant une année au moins puisqu'il faut un certain temps avant de s'apercevoir d'une violation et cela permet de donner aux enquêteurs un historique des informations de volume suffisant pour déterminer la durée d'une violation potentielle et du ou des systèmes éventuellement affectés. En gardant immédiatement à disposition les journaux des trois derniers mois au moins, une analyse peut rapidement identifier et minimiser l'impact d'une violation des données. Le stockage des journaux hors ligne peut empêcher qu'ils soient facilement accessibles à la lecture et provoquer des durées plus longues pour la restauration des données de journaux, la performance des analyses et l'identification des systèmes ou données affectés.</p>
<p>10.8 Condition supplémentaire pour les prestataires de services uniquement : Implémenter un processus pour détecter et signaler à temps les pannes des systèmes de contrôle de sécurité critiques, y compris, mais sans s'y limiter, les pannes relatives aux :</p> <ul style="list-style-type: none"> • Pare-feu • IDS/IPS • FIM • Antivirus • Contrôles d'accès physiques 	<p>10.8.a Examiner les politiques et les procédures pour vérifier que les processus sont définis pour détecter et signaler à temps les pannes des systèmes de contrôle de sécurité critiques, y compris, mais sans s'y limiter, les pannes relatives aux :</p> <ul style="list-style-type: none"> • Pare-feu • IDS/IPS • FIM • Antivirus • Contrôles d'accès physiques • Contrôles d'accès logiques • Mécanismes de journalisation d'audit • Contrôles de segmentation (le cas échéant) 	<p>Remarque : Cette condition ne s'applique que lorsque l'entité évaluée est un prestataire de services.</p> <p>À défaut de processus formels pour détecter et signaler les pannes de contrôles de sécurité critiques, les pannes peuvent ne pas être détectées pendant des périodes prolongées et peuvent procurer aux pirates tout le temps nécessaire pour compromettre les systèmes et pour voler des données confidentielles dans l'environnement des données de titulaires de carte.</p> <p>Les types spécifiques de pannes peuvent varier</p>

Conditions PCI DSS	Procédures de test	Directive
<ul style="list-style-type: none"> • Contrôles d'accès logiques • Mécanismes de journalisation d'audit • Contrôles de segmentation (le cas échéant) <p><i>Remarque : Cette condition est considérée comme une meilleure pratique jusqu'au 31 janvier 2018, après quoi ce sera une obligation.</i></p>	<p>10.8.b Examiner les processus de détection et d'alerte et interroger le personnel pour vérifier que les processus sont implémentés pour tous les contrôles de sécurité critiques et que la panne d'un tel contrôle se solde par le déclenchement d'une alerte.</p>	<p>selon la fonction du dispositif et la technologie utilisée. Les pannes types incluent ce qui suit : l'interruption de la fonction de sécurité par le système ou un dysfonctionnement, par exemple, l'effacement de toutes les règles par le pare-feu ou une mise hors tension.</p>
<p>10.8.1 Condition supplémentaire pour les prestataires de services uniquement : Intervenir face aux pannes de contrôles de sécurité critiques en temps opportun. Les processus de résolution des pannes de contrôles de sécurité doivent comprendre :</p> <ul style="list-style-type: none"> • Rétablissement des fonctions de sécurité • Identification et documentation de la durée (date et heure de début et de fin) de la panne de sécurité • Identification et documentation des causes de la panne, y compris la cause fondamentale, et documentation des rectificatifs requis pour résoudre la cause 	<p>10.8.1.a Examiner les politiques et les procédures documentées et interroger le personnel pour vérifier que les processus sont définis et mis en oeuvre pour résoudre une panne de contrôle de sécurité et qu'ils comprennent :</p> <ul style="list-style-type: none"> • Rétablissement des fonctions de sécurité • Identification et documentation de la durée (date et heure de début et de fin) de la panne de sécurité • Identification et documentation des causes de la panne, y compris la cause fondamentale, et documentation des rectificatifs requis pour résoudre la cause fondamentale • Identification et résolution des problèmes de sécurité survenus pendant la panne • Évaluation des risques pour déterminer si d'autres actions sont indispensables suite à une panne de sécurité • Implémentation des contrôles pour prévenir la répétition d'une telle panne • Reprise de la surveillance des contrôles de sécurité 	<p><i>Remarque : Cette condition ne s'applique que lorsque l'entité évaluée est un prestataire de services.</i></p> <p>Si les alertes relatives aux pannes des contrôles de sécurité critiques ne sont pas résolues rapidement et efficacement, les pirates peuvent profiter de la situation pour insérer des logiciels malveillants, prendre le contrôle d'un système ou voler des données dans l'environnement de l'entité.</p> <p>Les justificatifs documentés (par exemple, des registres dans un système de gestion des problèmes) doivent indiquer que des processus et des procédures sont mis en oeuvre pour résoudre les pannes de sécurité. Qui plus est, le personnel doit être conscient de ses responsabilités en cas</p>

Conditions PCI DSS	Procédures de test	Directive
<p>fondamentale</p> <ul style="list-style-type: none"> • Identification et résolution des problèmes de sécurité survenus pendant la panne • Évaluation des risques pour déterminer si d'autres actions sont indispensables suite à une panne de sécurité • Implémentation des contrôles pour prévenir la répétition d'une telle panne • Reprise de la surveillance des contrôles de sécurité <p><i>Remarque : Cette condition est considérée comme une meilleure pratique jusqu'au 31 janvier 2018, après quoi ce sera une obligation.</i></p>	<p>10.8.1.b Examiner les registres pour vérifier que les pannes des contrôles de sécurité sont documentées et comprennent ce qui suit :</p> <ul style="list-style-type: none"> • Identification des causes de la panne, y compris la cause fondamentale • Durée (date et heure de début et de fin) de la panne de sécurité • Détails de la résolution requise pour rectifier la cause fondamentale 	<p>de panne. Les mesures et les interventions relatives aux pannes doivent être présentées dans les justificatifs documentés.</p>
<p>10.9 Assurer que les politiques de sécurité et les procédures opérationnelles pour le contrôle de tous les accès aux ressources du réseau et aux données de titulaires de carte sont documentées, utilisées et connues de toutes les parties concernées.</p>	<p>10.9 Examiner la documentation et interroger le personnel pour vérifier que les politiques de sécurité et les procédures opérationnelles pour le contrôle de tous les accès aux ressources du réseau et aux données de titulaires de carte sont :</p> <ul style="list-style-type: none"> • Documentées • Utilisées et • Connues de toutes les parties concernées. 	<p>Le personnel doit être conscient et suivre les politiques de sécurité et les procédures opérationnelles quotidiennes pour la surveillance de tous les accès aux ressources du réseau et aux données de titulaires de carte sur une base continue.</p>

Condition 11 : Tester régulièrement les processus et les systèmes de sécurité

Des vulnérabilités sont sans cesse découvertes par des individus malveillants et des chercheurs, et sont introduites avec tout nouveau logiciel. Les composants de système, les processus et les logiciels personnalisés doivent être fréquemment testés afin de s'assurer que les contrôles de sécurité reflètent toujours les nouveaux environnements.

Conditions PCI DSS	Procédures de test	Directive
<p>11.1 Mettre en œuvre des processus pour tester la présence de points d'accès sans-fil (802.11) ; détecter et identifier tous les points d'accès sans-fil autorisés et non autorisés sur une base trimestrielle.</p> <p>Remarque : Les analyses de réseau sans-fil, les inspections logiques/physiques des composants de système et de l'infrastructure, le contrôle d'accès réseau (NAC) ou les systèmes de détection et/ou de prévention d'intrusions sans-fil sont quelques exemples de méthodes pouvant être utilisées pour ce processus.</p> <p>Quelles que soient les méthodes utilisées, elles doivent être suffisantes pour détecter et identifier les appareils autorisés ainsi que les appareils non autorisés.</p>	<p>11.1.a Examiner les politiques et les procédures pour vérifier que des processus sont définis pour la détection et l'identification des points d'accès sans-fil autorisés et non autorisés sur une base trimestrielle.</p> <p>11.1.b Vérifier que la méthodologie est appropriée et qu'elle permet de détecter et d'identifier tout point d'accès sans-fil non autorisé, notamment au moins ce qui suit :</p> <ul style="list-style-type: none"> • Cartes WLAN insérées dans les composants de système ; • Appareils portables ou mobiles reliés à un composant du système pour créer un point d'accès sans-fil (par exemple, par USB, etc.) ; • Des périphériques sans-fil branchés sur un port réseau ou à un périphérique réseau. <p>11.1.c Si la technologie sans fil est utilisée, examiner le résultat des scans de réseau sans fil récents pour vérifier que :</p> <ul style="list-style-type: none"> • Les points d'accès autorisés et non autorisés sont identifiés ; et • Le scan est effectué au moins une fois par trimestre pour tous les composants et toutes les installations du système. <p>11.1.d Si l'on utilise une surveillance automatisée (par exemple systèmes de détection et/ou de prévention d'intrusions sans-fil, NAC, etc.), vérifier que la configuration déclenchera des alertes pour informer le personnel.</p>	<p>La mise en œuvre et/ou l'exploitation de la technologie sans-fil sur un réseau font partie des voies les plus fréquentes utilisées par les utilisateurs malveillants pour accéder au réseau et aux données de titulaires de carte. Si un périphérique ou un réseau sans-fil est installé à l'insu d'une société, il peut permettre à un pirate de pénétrer facilement sur le réseau, à l'insu de tous. Des dispositifs sans-fil non autorisés peuvent être dissimulés dans, ou connectés à, un ordinateur ou à un autre composant du système, ou encore être directement connectés à un port ou à un dispositif du réseau, comme un commutateur ou un routeur. Un tel dispositif non autorisé peut constituer un point d'accès non autorisé à l'environnement.</p> <p>Savoir quels sont les appareils sans-fil qui sont autorisés peut aider les administrateurs à identifier rapidement les appareils non autorisés et répondre à l'identification de points d'accès sans-fil aide à minimiser de manière proactive l'exposition du CDE aux individus malveillants.</p> <p>En raison de la facilité avec laquelle un point d'accès sans-fil peut être connecté à un réseau, de la difficulté à détecter leur présence et du risque accru associé aux équipements sans-fil non autorisés, ces processus doivent être exécutés même s'il existe une politique interdisant l'usage de la technologie sans-fil.</p> <p>La taille et la complexité d'un environnement particulier déterminent les outils et processus appropriés à utiliser afin de fournir une garantie suffisante qu'un point d'accès mal intentionné n'a</p>

Conditions PCI DSS	Procédures de test	Directive
		<p>pas été installé dans l'environnement.</p> <p>(suite à la page suivante)</p>
<p>11.1.1 Maintenir un registre des points d'accès sans-fil autorisés comprenant une justification commerciale documentée.</p>	<p>11.1.1 Examiner les archives documentées pour vérifier qu'un registre des points d'accès sans-fil autorisés est maintenu et que la justification commerciale est documentée pour tous les points d'accès sans-fil documentés.</p>	<p>Par exemple : Dans le cas d'un simple terminal autonome dans un centre commercial, où tous les composants de communication sont contenus dans des boîtiers inviolables et, comportant des dispositifs pour rendre les effractions évidentes, une inspection physique détaillée du terminal lui-même peut suffire à s'assurer qu'aucun point d'accès frauduleux n'y a été branché ni installé. Cependant, dans un environnement comportant des nœuds multiples (comme un grand magasin de détail, un centre d'appels, une salle de serveur ou un centre de données), il est plus difficile d'effectuer une inspection physique détaillée. Dans ce cas, diverses méthodes peuvent être combinées afin de remplir les conditions, par exemple, effectuer des inspections physiques du système conjointement aux résultats d'un analyseur sans-fil.</p>
<p>11.1.2 Mettre en œuvre des procédures de réponse aux incidents au cas où des points d'accès non autorisés sont détectés.</p>	<p>11.1.2.a Examiner le plan de réponse aux incidents de l'organisation (Condition 12.10) pour vérifier qu'il définit et exige une réponse au cas où un point d'accès sans-fil non autorisé est détecté.</p> <p>11.1.2.b Interroger le personnel responsable et/ou inspecter les derniers scans de réseau sans-fil et les réponses connexes pour vérifier que des mesures sont prises lorsqu'un point d'accès sans-fil non autorisé est découvert.</p>	

Conditions PCI DSS	Procédures de test	Directive
<p>11.2 Analyser les vulnérabilités potentielles des réseaux internes et externes au moins une fois par trimestre et après tout changement significatif des réseaux (par exemple, installation de nouveaux composants de système, modification de la topologie du réseau ou des règles des pare-feu, mise à niveau de produits).</p> <p><i>Remarque : De multiples rapports de scan peuvent être combinés pour que le processus de scan trimestriel montre que tous les systèmes ont été scannés et que toutes les vulnérabilités applicables ont été traitées. Une documentation supplémentaire peut être requise pour vérifier que les vulnérabilités qui n'ont pas été résolues sont en phase de l'être.</i></p> <p><i>Pour la conformité initiale à la norme PCI DSS, il n'est pas obligatoire que quatre scans trimestriels aient été réalisées avec succès si l'évaluateur vérifie que 1) le résultat du dernier scan était réussi, 2) l'entité a documenté les politiques et les procédures exigeant l'exécution de scans trimestriels et 3) toutes les vulnérabilités relevées dans les résultats ont été corrigées, comme indiqué lors de la réexécution du scan. Pour les années qui suivent la vérification PCI DSS initiale, quatre scans trimestriels réussis ont été réalisées.</i></p>	<p>11.2 Examiner les rapports de scan et la documentation connexe pour vérifier que les scans de vulnérabilité internes et externes sont effectués comme suit :</p>	<p>Un scan de vulnérabilité est une combinaison d'outils, de techniques et/ou de méthodes automatisé(e)s ou manuel(le)s, exécuté(e)s sur les équipements et les serveurs internes et externes du réseau, conçu(e)s pour exposer les vulnérabilités potentielles qui pourraient être détectées et exploitées par des individus malveillants.</p> <p>Il existe trois types de scans de vulnérabilité requis pour la norme PCI DSS :</p> <ul style="list-style-type: none"> • Le scan de vulnérabilité interne trimestriel effectué par un personnel qualifié (l'utilisation d'un fournisseur de service de scan approuvé (ASV) n'est pas recommandée) • Le scan de vulnérabilité externe trimestriel, qui doit être effectué par un ASV. • Les scans internes et externes sont requis après tout changement d'importance. <p>Une fois ces faiblesses identifiées, l'organisation les corrige et répète le scan jusqu'à ce que toutes les vulnérabilités aient été corrigées.</p> <p>Identifier les vulnérabilités et y remédier en temps opportun réduit la probabilité qu'elles soient exploitées et permettent de compromettre un composant de système ou des données de titulaires de carte.</p>
<p>11.2.1 Effectuer des scans trimestriels de vulnérabilité interne. Résoudre les vulnérabilités et renouveler les scans</p>	<p>11.2.1.a Examiner les rapports d'analyse et vérifier que quatre analyses trimestrielles internes ont eu lieu au cours de la période de 12 mois la plus récente.</p>	<p>Un processus établi d'identification des vulnérabilités sur des systèmes internes exige que les scans de vulnérabilité soient effectués</p>

Conditions PCI DSS	Procédures de test	Directive
<p>pour vérifier que toutes les vulnérabilités à « risque élevé » sont résolues conformément à la classe de vulnérabilité de l'entité (selon la condition 6.1). Les analyses doivent être exécutées par un personnel qualifié.</p>	<p>11.2.1.b Examiner les rapports de scan, vérifier que toutes les vulnérabilités à « haut risque » sont résolues et que le processus d'analyse comprend des nouveaux scans pour vérifier que toutes les vulnérabilités à « haut risque » (comme défini dans la condition 6.1 de la norme PCI DSS) sont résolues.</p> <p>11.2.1.c Interroger le personnel pour vérifier que le scan a été effectué par une ressource interne ou un tiers externe qualifié et, le cas échéant, que le testeur appartient à une organisation indépendante (il ne doit pas obligatoirement être un QSA ou un ASV).</p>	<p>trimestriellement. Les vulnérabilités constituant le risque le plus important pour l'environnement (par exemple, celles classées à « haut risque » aux termes de la condition 6.1) doivent être résolues en priorité absolue.</p> <p>Les scans de vulnérabilité interne peuvent être exécutés par un personnel interne qualifié, raisonnablement indépendant du ou des composants de système analysés (par exemple, un administrateur de pare-feu ne doit pas être chargé du scan de pare-feu), ou une entreprise peut choisir de faire exécuter ces scans de vulnérabilité interne par un prestataire de services spécialisé dans l'analyse des vulnérabilités.</p>
<p>11.2.2 Des analyses de vulnérabilité externe doivent être effectuées une fois par trimestre par un prestataire de services de scan agréé par le PCI SSC (Payment Card Industry Security Standards Council - Conseil des normes de sécurité PCI). Recommencer le scan si nécessaire, jusqu'à ce que les scans soient réussis.</p> <p>Remarque : Les scans de vulnérabilité externe doivent être effectués une fois par trimestre par un prestataire de services de scan agréé (ASV) par le PCI SSC (Payment Card Industry Security Standards Council - Conseil des normes de sécurité PCI).</p> <p>Consulter le Guide de programme ASV publié sur le site Web du PCI SSC pour connaître les responsabilités du client vis-à-vis du scan, la préparation du scan, etc.</p>	<p>11.2.2.a Examiner les résultats des quatre scans trimestriels de vulnérabilité externe les plus récents et vérifier qu'ils ont tous eu lieu au cours des 12 derniers mois.</p> <p>11.2.2.b Examiner les résultats de chacun des quatre scans trimestriels pour s'assurer qu'ils satisfont aux conditions du guide de programme ASV (par exemple, pas de vulnérabilité supérieure à la note 4.0 du CVSS et aucune défaillance automatique).</p> <p>11.2.2.c Examiner les rapports de scan pour vérifier que les scans ont été réalisés par un prestataire de services de scan agréé (ASV) par le PCI SSC.</p>	<p>Les réseaux externes étant plus exposés, le scan trimestriel de vulnérabilités externes doit être exécuté par un prestataire de services d'analyse agréé (ASV) par le PCI SSC.</p> <p>Un programme d'analyse fiable garantit que les scans sont réalisés et les vulnérabilités traitées en temps opportun.</p>

Conditions PCI DSS	Procédures de test	Directive
<p>11.2.3 Effectuer les scans internes et externes et recommencez si nécessaire, après tout changement d'importance. Les analyses doivent être exécutées par un personnel qualifié.</p>	<p>11.2.3.a Inspecter et mettre en corrélation la documentation de changement de contrôle et les rapports de scan afin de vérifier que les composants de système sujets à un changement d'importance ont été scannés.</p> <p>11.2.3.b Examiner les rapports d'analyse et vérifier que le processus d'analyse stipule de nouvelles analyses jusqu'à ce que :</p> <ul style="list-style-type: none"> • Pour les scans externes, aucune vulnérabilité supérieure à la note 4.0 du CVSS n'existe. • Pour les scans internes, toutes les vulnérabilités à « haut risque », définies dans la condition 6.1 de la norme PCI DSS, sont résolues. <p>11.2.3.c Confirmer que le scan a été effectué par une ressource interne ou un tiers externe qualifié et, le cas échéant, que le testeur appartient à une organisation indépendante (il ne doit pas obligatoirement être un QSA ou un ASV).</p>	<p>Déterminer ce qui constitue un changement significatif dépend considérablement de la configuration d'un environnement donné. Si une mise à jour ou une modification touche uniquement les données de titulaires de carte ou affecte la sécurité de l'environnement de données de titulaires de carte, elle doit être considérée comme significative.</p> <p>L'analyse d'un environnement, après avoir apporté des modifications d'importance à ce dernier, garantit que les modifications ont été réalisées de la manière appropriée et que la sécurité de l'environnement n'a pas été compromise à la suite de ces modifications. Tous les composants de système affectés par les modifications doivent être scannés.</p>
<p>11.3 Mettre en œuvre une méthodologie pour le test de pénétration qui inclut ce qui suit :</p> <ul style="list-style-type: none"> • Se base sur les approches de test de pénétration acceptées par l'industrie (par exemple NIST SP800-115) • Recouvre la totalité du périmètre du CDE ainsi que les systèmes critiques • Comprend un test depuis l'intérieur et l'extérieur du système • Comprend un test pour valider tout contrôle de segmentation et de réduction de la portée. • Définit les tests de pénétration de couche d'application pour qu'ils 	<p>11.3 Examiner la méthodologie de test de pénétration et interroger le personnel responsable pour vérifier qu'une méthodologie est mise en œuvre qui comprend les points suivants :</p> <ul style="list-style-type: none"> • Se base sur les approches de test de pénétration acceptées par l'industrie (par exemple NIST SP800-115) • Recouvre la totalité du périmètre du CDE ainsi que les systèmes critiques • Test depuis l'intérieur et l'extérieur du système • Comprend un test pour valider tout contrôle de segmentation et de réduction de la portée. • Définit les tests de pénétration de couche d'application pour qu'ils comprennent, au minimum les vulnérabilités indiquées dans la Condition 6.5. • Définit les tests de pénétration de couche d'application 	<p>L'objectif d'un test de pénétration est de simuler une attaque en conditions réelles dans le but d'identifier jusqu'où un pirate pourrait pénétrer dans un environnement donné. Ceci permet à une entreprise d'avoir une meilleure compréhension de son exposition éventuelle au risque et de développer une stratégie de défense contre les attaques.</p> <p>Un test de pénétration diffère d'un scan de vulnérabilité, dans la mesure où le test de pénétration est un processus actif pouvant comprendre l'exploitation de vulnérabilités identifiées. Exécuter un scan de vulnérabilité peut être l'une des premières étapes effectuées par le test de pénétration afin de planifier la stratégie de test, bien que ce ne soit pas la seule étape. Même</p>

Conditions PCI DSS	Procédures de test	Directive
<p>comprennent, au minimum les vulnérabilités indiquées dans la Condition 6.5.</p> <ul style="list-style-type: none"> • Définit les tests de pénétration de couche d'application pour qu'ils comprennent les composants qui prennent en charge les fonctions réseau, tels que les systèmes d'exploitation. • Comprend l'examen et la prise en compte des menaces et des vulnérabilités subies au cours des 12 derniers mois • Spécifie la rétention des résultats de test de pénétration et les résultats des activités de réparation. 	<p>pour qu'ils comprennent les composants qui prennent en charge les fonctions réseau, tels que les systèmes d'exploitation.</p> <ul style="list-style-type: none"> • Comprend l'examen et la prise en compte des menaces et des vulnérabilités subies au cours des 12 derniers mois • Spécifie la rétention des résultats de test de pénétration et les résultats des activités de réparation. 	<p>si le scan de vulnérabilité ne détecte pas de vulnérabilités connues, la personne exécutant le test de pénétration obtiendra suffisamment d'informations sur le système pour identifier les lacunes éventuelles dans la sécurité.</p> <p>Le test de pénétration est généralement un processus en grande partie manuel. Bien qu'il soit possible d'utiliser certains outils automatisés, la personne réalisant le test doit utiliser sa connaissance des systèmes pour pénétrer dans un environnement. Souvent elle appliquera plusieurs types d'exploits ensemble dans le but de franchir plusieurs couches de défenses. Par exemple, si elle trouve un moyen d'accéder à un serveur d'application, elle utilisera ensuite le serveur compromis comme point de départ pour lancer une nouvelle attaque en fonction des ressources auxquelles le serveur a accès. De cette manière, la personne effectuant le test est en mesure de simuler les méthodes utilisées par un pirate afin d'identifier les zones de faiblesse potentielles dans l'environnement.</p> <p><i>Les techniques de test de pénétration seront différentes pour les différentes organisations et le type, la profondeur et la complexité des tests dépendront de l'environnement spécifique et de l'évaluation des risques de l'organisation.</i></p>
<p>11.3.1 Effectuer des tests de pénétration <i>externe</i> au moins une fois par an et après tout changement ou mise à niveau significatif de l'infrastructure ou de l'application (par exemple, mise à niveau du système d'exploitation ou ajout d'un sous-réseau ou d'un serveur Web dans l'environnement).</p>	<p>11.3.1.a Examiner le champ d'application du travail et les résultats du dernier test de pénétration externe pour vérifier qu'un tel test est effectué comme suit :</p> <ul style="list-style-type: none"> • Selon la méthodologie définie • Au moins une fois par an ; • Après les changements significatifs de l'environnement. <p>11.3.1.c Vérifier que le test a été effectué par une ressource interne ou un tiers externe qualifié et, le cas échéant, que l'organisation du testeur est bien indépendante (ne doit pas obligatoirement être un QSA ou un ASV).</p>	<p>Les tests de pénétration effectués régulièrement et après les changements significatifs apportés à l'environnement constituent une mesure de sécurité proactive qui aide à minimiser les risques d'accès potentiel au CDE par des individus malveillants.</p> <p>Déterminer ce qui constitue un changement ou significatif ou une mise à jour significative dépend considérablement de la configuration d'un environnement donné. Si une mise à jour ou une modification touche uniquement les données de</p>

Conditions PCI DSS	Procédures de test	Directive
<p>11.3.2 Effectuer des tests de pénétration <i>internes</i> au moins une fois par an et après tout changement ou mise à niveau significatif de l'infrastructure ou de l'application (par exemple, mise à niveau du système d'exploitation ou ajout d'un sous-réseau ou d'un serveur Web dans l'environnement).</p>	<p>11.3.2.a Examiner le champ d'application du travail et les résultats du dernier test de pénétration interne pour vérifier qu'un tel test est effectué comme suit :</p> <ul style="list-style-type: none"> • Selon la méthodologie définie • Au moins une fois par an ; • Après les changements significatifs de l'environnement. <p>11.3.2.b Vérifier que le test a été effectué par une ressource interne ou un tiers externe qualifié et, le cas échéant, que l'organisation du testeur est bien indépendante (ne doit pas obligatoirement être un QSA ou un ASV).</p>	<p>titulaires de carte ou affecte la sécurité de l'environnement de données de titulaires de carte, elle doit être considérée comme significative. Les tests de pénétration après les mises à jour et les modifications du réseau permettent d'assurer que tous les contrôles en place fonctionnent toujours aussi efficacement après le déploiement de la mise à niveau ou de la modification.</p>
<p>11.3.3 Les vulnérabilités exploitables découvertes pendant le test de pénétration sont corrigées et les tests sont recommencés pour vérifier les corrections.</p>	<p>11.3.3 Examiner les résultats de test de pénétration pour vérifier que les vulnérabilités exploitables ont été corrigées et que les nouveaux tests ont confirmés que la vulnérabilité a été corrigée.</p>	

Conditions PCI DSS	Procédures de test	Directive
<p>11.3.4 Si la segmentation est utilisée pour isoler le CDE des autres réseaux, effectuer des tests de pénétration au moins une fois par an et après toute modification des méthodes/contrôles de segmentation pour vérifier que les méthodes de segmentation sont opérationnelles et efficaces, et isoler tous les systèmes hors champ d'application des systèmes inclus dans le CDE.</p>	<p>11.3.4.a Examiner les contrôles de segmentation et examiner la méthodologie de test de pénétration pour vérifier que les procédures de test de pénétration sont définies pour qu'elles testent toutes les méthodes de segmentation afin de confirmer qu'elles sont opérationnelles et efficaces, et isoler tous les systèmes hors champ d'application des systèmes inclus dans le CDE.</p>	<p>Les tests de pénétration sont un outil important pour confirmer que toutes les segmentations en place pour isoler le CDE des autres réseaux sont efficaces. Les tests de pénétration doivent se concentrer sur les contrôles de segmentation, à la fois depuis l'extérieur du réseau de l'entité et de l'intérieur du réseau, mais hors du CDE, pour confirmer qu'ils ne peuvent pas passer les contrôles de segmentation pour accéder au CDE. Par exemple, les tests de réseau et/ou les scans de ports ouverts pour vérifier l'absence de connectivité entre les réseaux dans la portée et les réseaux hors champ d'application.</p>
	<p>11.3.4.b Examiner les résultats du dernier test de pénétration pour vérifier ce qui suit :</p> <ul style="list-style-type: none"> • Le test de pénétration destiné à vérifier les contrôles de segmentation est réalisé au moins une fois par an et après toute modification aux contrôles/méthodes de segmentation. • Le test de pénétration couvre tous les contrôles/toutes les méthodes de segmentation utilisé(e)s. • Le test de pénétration vérifie que les contrôles/méthodes de segmentation sont opérationnel(le)s et efficaces, et isole tous les systèmes hors de portée des systèmes dans le CDE. 	
	<p>11.3.4.c Vérifier que le test a été effectué par une ressource interne ou un tiers externe qualifié(e) et, le cas échéant, que l'indépendance opérationnelle du testeur existe réellement (il ne doit pas obligatoirement être un QSA ou un ASV).</p>	

Conditions PCI DSS	Procédures de test	Directive
<p>11.3.4.1 Condition supplémentaire pour les prestataires de services uniquement : En cas de segmentation, confirmer le champ d'application de la norme PCI DSS en effectuant des tests de pénétration sur les contrôles de segmentation au moins une fois par semestre et après des modifications apportées aux contrôles/méthodes de segmentation.</p> <p><i>Remarque</i> : Cette condition est considérée comme une meilleure pratique jusqu'au 31 janvier 2018, après quoi ce sera une obligation.</p>	<p>11.3.4.1.a Examiner les résultats du dernier test de pénétration externe pour vérifier ce qui suit :</p> <ul style="list-style-type: none"> Le test de pénétration est effectué pour vérifier les contrôles de segmentation au moins une fois par semestre et après des modifications apportées aux contrôles/méthodes de segmentation. Le test de pénétration couvre tous les contrôles/toutes les méthodes de segmentation utilisées. Le test de pénétration vérifie que les contrôles/méthodes de segmentation sont opérationnel(le)s et efficaces, et isole tous les systèmes hors de portée des systèmes dans le CDE. 	<p>Remarque : Cette condition ne s'applique que lorsque l'entité évaluée est un prestataire de services.</p> <p>Pour les prestataires de services, le champ d'application de la norme PCI DSS doit être validé aussi fréquemment que possible pour en assurer la tenue à jour et la mise en correspondance avec les objectifs commerciaux en constante évolution.</p>
	<p>11.3.4.1.b Vérifier que le test a été effectué par une ressource interne ou un tiers externe qualifié et, le cas échéant, que l'indépendance opérationnelle du testeur existe réellement (il ne doit pas obligatoirement être un QSA ou un ASV).</p>	
<p>11.4 Utiliser les techniques d'intrusion-détection et/ou d'intrusion-prévention pour détecter et/ou empêcher les intrusions dans le réseau. Surveiller la totalité du trafic au périmètre de l'environnement de données de titulaires de carte, ainsi qu'aux points critiques de l'environnement des données de titulaires de carte et alerter le personnel en cas de soupçons de compromis.</p> <p>Tenir à jour tous les moteurs d'intrusion-détection et de prévention, les lignes de base et les signatures.</p>	<p>11.4.a Examiner les configurations de système et les diagrammes de réseau pour vérifier que des techniques (telles que les systèmes d'intrusion-détection et/ou des systèmes d'intrusion/prévention) sont en place pour la surveillance du trafic :</p> <ul style="list-style-type: none"> Au périmètre de l'environnement de données de titulaires de carte ; Aux points critiques de l'environnement de données de titulaires de carte. <p>11.4.b Examiner les configurations du système et interroger le personnel responsable pour confirmer que les techniques d'intrusion-détection et/ou d'intrusion-prévention alertent le personnel en cas de soupçon de compromis.</p>	<p>Les techniques de détection d'intrusion et/ou de prévention d'intrusion (telles que IDS/IPS) comparent le trafic entrant sur le réseau avec des « signatures » connues et/ou des comportements de milliers de types de violations (outils de piratage, chevaux de Troie et autres logiciels malveillants), envoient des alertes et/ou bloquent la tentative. Sans une approche proactive à la détection des activités non autorisées, les attaques (ou l'utilisation frauduleuse) des ressources d'un ordinateur pourraient passer inaperçues au moment où elles se produisent. Les alertes de sécurité générées par ces techniques doivent être surveillées de manière à pouvoir bloquer les</p>

Conditions PCI DSS	Procédures de test	Directive
	<p>11.4.c Examiner les configurations IDS/IPS et la documentation du fournisseur pour vérifier que les techniques d'intrusion/détection et/ou d'intrusion/prévention sont configurées, maintenues et mises à jour selon les instructions du fournisseur afin d'assurer une protection optimale.</p>	tentatives d'intrusion.
<p>11.5 Déployer des mécanismes de détection des modifications (par exemple, des outils de contrôle de l'intégrité des fichiers) pour alerter le personnel de toute modification non autorisée (y compris des changements, des ajouts et des suppressions) des fichiers critiques du système, des fichiers de configuration ou des fichiers de contenu et configurer le logiciel pour qu'il effectue des comparaisons de fichier critique au moins une fois par semaine.</p> <p style="text-align: right;"><i>(suite à la page suivante)</i></p> <p>Remarque : <i>Pour la détection des changements, les fichiers critiques sont généralement ceux qui ne changent pas régulièrement, mais dont la modification pourrait indiquer une altération du système ou son exposition à des risques. Les mécanismes de détection des changements tels que les produits de surveillance d'intégrité de fichier sont généralement préconfigurés avec les fichiers critiques pour le système d'exploitation connexe. D'autres fichiers stratégiques, tels que ceux associés aux applications personnalisées, doivent être évalués et définis par l'entité (c'est-à-dire le commerçant ou le prestataire de services).</i></p>	<p>11.5.a Vérifier l'utilisation de mécanismes de détection des modifications en examinant les paramètres système et les fichiers contrôlés, ainsi que les résultats des activités de contrôle.</p> <p>Exemples de fichiers qui doivent être contrôlés :</p> <ul style="list-style-type: none"> • Exécutables du système ; • Exécutables des applications ; • Fichiers de configuration et de paramètres ; • Fichiers d'historique, d'archive, de registres et d'audit stockés à un emplacement centralisé. • Les fichiers critiques supplémentaires déterminés par l'entité (par exemple, avec l'évaluation de risque ou par d'autres moyens). <p>11.5.b Vérifier que le mécanisme est configuré de manière à alerter le personnel de toute modification non autorisée (y compris les changements, les ajouts et les suppressions) des fichiers critiques, et à procéder aux comparaisons de fichiers critiques au moins une fois par semaine.</p>	<p>Les solutions de détection des modifications, comme les outils de contrôle de l'intégrité des fichiers (file-integrity monitoring, FIM), vérifient les changements, les ajouts et les suppressions des fichiers critiques, et signalent quand de telles modifications sont détectées. Si elles ne sont pas mises en œuvre correctement et que les résultats de la solution de détection des modifications sont contrôlés, un individu malveillant pourrait ajouter, supprimer ou altérer les contenus de fichier de configuration, les programmes du système d'exploitation ou les exécutables d'application. Les modifications non autorisées, si elles ne sont pas détectées, peuvent rendre inutiles les contrôles de sécurité existants et/ou aboutir au vol des données de titulaires de carte sans aucun impact perceptible au niveau du traitement normal.</p>

Conditions PCI DSS	Procédures de test	Directive
<p>11.5.1 Mettre en œuvre un processus pour répondre à n'importe quelle alerte générée par la solution de détection de changement.</p>	<p>11.5.1 Interroger le personnel pour vérifier que les alertes sont contrôlées et résolues.</p>	
<p>11.6 Assurer que les politiques de sécurité et les procédures opérationnelles pour la surveillance et les tests de sécurité sont documentées, utilisées et connues de toutes les parties concernées.</p>	<p>11.6 Examiner la documentation et interroger le personnel pour vérifier que les politiques de sécurité et les procédures opérationnelles pour le contrôle et les tests de sécurité sont :</p> <ul style="list-style-type: none"> • Documentées, • Utilisées et • Connues de toutes les parties concernées. 	<p>Le personnel doit être conscient et suivre les politiques de sécurité et les procédures opérationnelles pour la surveillance et les tests de sécurité sur une base continue.</p>

Gestion d'une politique de sécurité des informations

Condition 12 : Maintenir une politique qui adresse les informations de sécurité pour l'ensemble du personnel

Une politique de sécurité robuste définit la sécurité mise en œuvre à l'échelle de l'entreprise et indique aux employés ce que l'on attend d'eux. Tout le personnel doit être sensibilisé au caractère confidentiel des données et à ses responsabilités dans la protection de ces informations. Dans le cadre de cette condition 12, le terme « personnel » désigne les employés à temps plein et à temps partiel, les intérimaires ainsi que les sous-traitants et les consultants qui « résident » sur le site de l'entité ou ont accès d'une manière ou d'une autre à l'environnement des données de titulaires de carte.

Conditions PCI DSS	Procédures de test	Directive
12.1 Établir, publier, maintenir et diffuser une politique de sécurité.	12.1 Passer en revue la politique de sécurité des informations et vérifier qu'elle est publiée et diffusée à tout le personnel concerné (mais aussi aux fournisseurs et partenaires commerciaux).	La politique de sécurité des informations d'une entreprise génère la feuille de route de l'application des mesures de sécurité afin de protéger ses ressources les plus précieuses. Tout le personnel doit être sensibilisé au caractère confidentiel des données et à ses responsabilités dans la protection de ces informations.
12.1.1 Examiner la politique de sécurité au moins une fois par an et mettre la politique à jour lorsque l'environnement change.	12.1.1 Vérifier que la politique de sécurité des informations est passée en revue au moins une fois par an et mise à jour le cas échéant, pour tenir compte des modifications apportées aux objectifs de l'entreprise ou à l'environnement de risque.	Les menaces à la sécurité et les méthodes de protection évoluent rapidement. Sans une mise à jour de la politique de sécurité afin de refléter ces changements, les nouvelles mesures de protection contre ces menaces sont inutiles.
12.2 Mettre en œuvre un processus d'évaluation des risques qui : <ul style="list-style-type: none"> Est effectué au moins une fois par an et à la suite des changements significatifs apportés à l'environnement (par exemple acquisition, intégration, déménagement, 	12.2.a Vérifier qu'un processus annuel d'évaluation des risques est documenté et : <ul style="list-style-type: none"> Identifie les actifs critiques, les menaces et les vulnérabilités. Se solde par une analyse formelle et documentée de risques. 	Une évaluation des risques permet à une organisation d'identifier les menaces et les vulnérabilités associées, pouvant avoir un impact négatif sur son activité. Exemples de facteurs à considérer en matière de risques : cybercriminalité, attaques Web et logiciels

Conditions PCI DSS	Procédures de test	Directive
<p>etc.)</p> <ul style="list-style-type: none"> Identifie les actifs critiques, les menaces et vulnérabilités, et Se solde par une analyse formelle et documentée de risques. <p><i>Les exemples de méthodologies d'évaluation des risques comprennent entre autres les directives OCTAVE, ISO 27005 et NIST SP 800-30.</i></p>	<p>12.2.b Examiner la documentation d'évaluation des risques, afin de vérifier que le processus d'évaluation des risques est exécuté au moins une fois par an et suite aux changements significatifs de l'environnement.</p>	<p>malveillants POS. Des ressources peuvent alors être effectivement affectées pour mettre en place des contrôles qui réduisent la probabilité et/ou l'impact potentiel de la menace.</p> <p>Effectuer des évaluations du risque au moins une fois par an et suite aux changements significatifs permet à l'organisation de rester à jour en ce qui concerne les changements organisationnels et l'évolution des menaces, des tendances et des technologies.</p>
<p>12.3 Développer les politiques d'utilisation des technologies critiques et définir l'utilisation adéquate de ces technologies.</p> <p><i>Remarque : Les exemples de technologies critiques comprennent notamment l'accès à distance et les technologies sans-fil, les ordinateurs portables, les tablettes, les supports électroniques amovibles, l'utilisation d'e-mail et d'Internet.</i></p> <p>S'assurer que ces politiques d'utilisation exigent ce qui suit :</p>	<p>12.3 Examiner les politiques d'utilisation des technologies critiques et interroger le personnel responsable pour vérifier que les politiques suivantes sont mises en œuvre et respectées :</p>	<p>Les politiques d'utilisation par le personnel peuvent interdire l'usage de certains équipements et autres technologies si c'est la politique de la société, ou donner au personnel des directives d'utilisation et d'application appropriées. Si ces politiques d'utilisation n'existent pas, le personnel peut utiliser des technologies enfreignant la politique de la société, permettant ainsi à des individus malveillants d'accéder aux systèmes stratégiques et aux données de titulaires de carte.</p>
<p>12.3.1 Approbation explicite des responsables</p>	<p>12.3.1 Vérifier que les politiques d'utilisation comprennent des processus pour l'approbation explicite des parties autorisées pour l'utilisation des technologies.</p>	<p>Si l'approbation appropriée d'application de ces technologies n'est pas exigée, un employé peut, en toute innocence, installer une solution dont il estime avoir besoin pour son activité, mais ouvrir en même temps une brèche importante qui expose les données et les systèmes stratégiques à des individus malveillants.</p>
<p>12.3.2 Authentification pour l'utilisation des technologies</p>	<p>12.3.2 Vérifier que les politiques d'utilisation comprennent des processus pour que toute utilisation de la technologie soit identifiée avec l'ID utilisateur et le mot de passe, ou tout autre élément d'identification (par exemple, un jeton).</p>	<p>Si la technologie est mise en œuvre sans une authentification appropriée (ID utilisateur et mots de passe, jetons, VPN, etc.), des individus malveillants peuvent facilement utiliser cette technologie non protégée pour accéder aux systèmes stratégiques et aux données de titulaires de carte.</p>

Conditions PCI DSS	Procédures de test	Directive
<p>12.3.3 Liste de tous les périphériques et du personnel disposant d'un accès</p>	<p>12.3.3 Vérifier que les politiques d'utilisation définissent :</p> <ul style="list-style-type: none"> • Une liste de tous les dispositifs critiques. • Une liste du personnel autorisé à utiliser ces dispositifs. 	<p>Des individus malveillants peuvent violer la sécurité physique et placer leurs propres équipements sur le réseau sous forme de « porte dérobée ». Le personnel peut également contourner les procédures et installer ses propres dispositifs. L'inventaire précis des équipements, avec un étiquetage approprié, permet d'identifier rapidement les installations non approuvées.</p>
<p>12.3.4 Une méthode permettant de déterminer rapidement et avec précision le propriétaire, les coordonnées et le but (par exemple, étiquetage, codage, et/ou inventaire des appareils)</p>	<p>12.3.4 Vérifier que les politiques d'utilisation définissent une méthode pour déterminer rapidement et avec précision le propriétaire, les coordonnées et le but (par exemple, étiquetage, codage, et/ou inventaire des appareils)</p>	<p>Des individus malveillants peuvent violer la sécurité physique et placer leurs propres équipements sur le réseau sous forme de « porte dérobée ». Le personnel peut également contourner les procédures et installer ses propres dispositifs. L'inventaire précis des équipements, avec un étiquetage approprié, permet d'identifier rapidement les installations non approuvées. Envisager d'établir une convention de dénomination officielle des appareils et de consigner tous les appareils aux contrôles d'inventaires mis en place. L'étiquetage logique peut être utilisé pour des informations comme des codes pouvant établir le lien entre un dispositif et son propriétaire, indiquer ses coordonnées et son objectif.</p>
<p>12.3.5 Usages acceptables de la technologie</p>	<p>12.3.5 Vérifier que les politiques d'utilisation définissent les utilisations acceptables de la technologie.</p>	<p>En définissant l'usage professionnel acceptable et l'emplacement des équipements et des technologies approuvés par la société, cette dernière pourra mieux gérer et contrôler les failles des configurations et des contrôles opérationnels, afin de s'assurer qu'aucune « porte dérobée » n'est ouverte pour permettre l'accès d'un individu malveillant aux systèmes stratégiques et aux données de titulaires de carte.</p>
<p>12.3.6 Emplacements acceptables des technologies sur le réseau</p>	<p>12.3.6 Vérifier que les politiques d'utilisation définissent les emplacements acceptables des technologies sur le réseau.</p>	
<p>12.3.7 Liste des produits approuvés par la société</p>	<p>12.3.7 Vérifier que les politiques d'utilisation comprennent une liste des produits approuvés par la société.</p>	

Conditions PCI DSS	Procédures de test	Directive
<p>12.3.8 Déconnexion automatique des sessions des technologies d'accès à distance après une période d'inactivité spécifique</p>	<p>12.3.8.a Vérifier que les politiques d'utilisation exigent la déconnexion automatique des sessions des technologies d'accès à distance après une période d'inactivité spécifique.</p>	<p>Les technologies d'accès à distance constituent souvent des « portes dérobées » vers les ressources stratégiques et données de titulaires de carte. Déconnecter ces technologies à distance lorsqu'elles ne sont pas utilisées (par exemple, celles qui sont utilisées pour la maintenance des systèmes par les fournisseurs de POS et autres ou les partenaires commerciaux), permet de réduire l'accès au réseau et le risque afférent.</p>
	<p>12.3.8.b Examiner les configurations des technologies d'accès à distance pour vérifier que les sessions d'accès à distance sont automatiquement déconnectées après une période d'inactivité spécifique.</p>	
<p>12.3.9 Activation des technologies d'accès à distance pour les fournisseurs et les partenaires commerciaux, uniquement lorsque c'est nécessaire, avec désactivation immédiate après usage</p>	<p>12.3.9 Vérifier que les politiques d'utilisation exigent l'activation des technologies d'accès à distance utilisées par les fournisseurs et partenaires commerciaux, uniquement lorsque c'est nécessaire, avec désactivation immédiate après usage.</p>	

Conditions PCI DSS	Procédures de test	Directive
<p>12.3.10 Lors de l'accès du personnel aux données de titulaires de carte au moyen de technologies d'accès à distance, interdire la copie, le déplacement et le stockage de données de titulaires de carte sur des disques durs locaux et des supports électroniques amovibles, sauf autorisation expresse pour un besoin professionnel défini.</p> <p>Lorsqu'il existe un besoin professionnel autorisé, la politique d'utilisation doit exiger que les données soient protégées selon toutes les conditions applicables de la norme PCI DSS.</p>	<p>12.3.10.a Vérifier que les politiques d'utilisation interdisent la copie, le déplacement ou le stockage des données de titulaires de carte sur des disques durs locaux et des supports électroniques amovibles lors de l'accès à ces informations au moyen de technologies d'accès à distance.</p> <p>12.3.10.b Pour le personnel dûment autorisé, vérifier que les politiques d'utilisation exigent la protection des données de titulaires de carte conformément aux conditions de la norme PCI DSS.</p>	<p>Pour assurer que l'ensemble du personnel est conscient qu'il ne doit pas stocker ni copier les données de titulaires de carte sur un ordinateur local personnel ni sur aucun autre support, votre politique doit clairement interdire ces activités, sauf pour le personnel qui y est expressément autorisé. Le stockage ou la copie des données de titulaires de carte sur un disque dur local ou un autre support doit être effectué conformément à toutes les conditions applicables de la norme PCI DSS.</p>
<p>12.4 S'assurer que la politique et les procédures de sécurité définissent clairement les responsabilités de tout le personnel en matière de sécurité.</p>	<p>12.4.a Vérifier que les politiques de sécurité des informations définissent clairement les responsabilités de tout le personnel en matière de sécurité.</p> <p>12.4.b Interroger un échantillon du personnel responsable pour vérifier qu'il comprend les politiques de sécurité.</p>	<p>Sans une définition claire des responsabilités et des rôles en matière de sécurité, l'interaction avec le groupe chargé de la sécurité peut être incohérente, conduisant alors au déploiement non sécurisé de technologies ou à l'usage de technologies obsolètes ou non sécurisées.</p>
<p>12.4.1 Condition supplémentaire pour les prestataires de services uniquement : L'équipe de direction a défini la responsabilité relative à la protection des</p>	<p>12.4.1.a Examiner la documentation pour vérifier que l'équipe de direction a affecté une responsabilité globale relative au respect de la conformité à la norme PCI DSS de l'entité.</p>	<p>Remarque : Cette condition ne s'applique que lorsque l'entité évaluée est un prestataire de services.</p>

Conditions PCI DSS	Procédures de test	Directive
<p>données de titulaires de carte et un programme de conformité à la norme PCI DSS, comme suit :</p> <ul style="list-style-type: none"> Responsabilité globale pour respecter la conformité à la norme PCI DSS Définition d'une charte pour un programme de conformité à la norme PCI DSS et des canaux de communication avec la direction <p><i>Remarque : Cette condition est considérée comme une meilleure pratique jusqu'au 31 janvier 2018, après quoi ce sera une obligation.</i></p>	<p>12.4.1.b Examiner la charte PCI DSS de la société pour vérifier si elle décrit les conditions propres au programme de conformité à la norme PCI DSS et les canaux de communication avec l'équipe de direction.</p>	<p>L'affectation de responsabilités relatives à la conformité à la norme PCI DSS par l'équipe de direction assure une visibilité optimale du programme de conformité à la norme PCI DSS et permet de poser les questions pertinentes pour déterminer l'efficacité du programme et influencer les priorités stratégiques. La responsabilité globale du programme de conformité à la norme PCI DSS peut être affectée à des rôles individuels et/ou aux divisions au sein de l'organisation.</p> <p>L'équipe de direction peut inclure des postes de niveau C, le Conseil d'administration ou autre unité équivalente. Les titres spécifiques dépendront de la structure organisationnelle concernée. Le niveau de détail fourni à l'équipe de direction doit varier en fonction de l'organisation concernée et du public visé.</p>
<p>12.5 Attribuer à un individu ou à une équipe les responsabilités suivantes de gestion de la sécurité des informations :</p>	<p>12.5 Examiner les politiques et les procédures concernant la sécurité pour vérifier :</p> <ul style="list-style-type: none"> L'assignation formelle de la sécurité des informations à un chef de la sécurité ou tout autre membre compétent de la direction. Les responsabilités suivantes de gestion de la sécurité des informations sont attribuées de manière spécifique et formelle : 	<p>Chaque individu ou équipe responsable de la gestion de la sécurité des informations doit avoir parfaitement conscience de ses responsabilités et des tâches associées, grâce à une politique spécifique. Sans cette responsabilisation, les lacunes dans les processus peuvent donner accès aux ressources stratégiques et aux données de titulaires de carte.</p>
<p>12.5.1 Définir, documenter et diffuser les politiques et les procédures de sécurité.</p>	<p>12.5.1 Vérifier que la responsabilité de l'établissement, de la documentation et de la distribution des procédures et politiques de sécurité est formellement attribuée.</p>	<p>Les entités doivent également prévoir des plans de transition et/ou de succession pour le personnel clé afin d'éviter toute faille des affectations de sécurité. En effet, une telle situation peut se solder par un manque d'affectation et d'exécution des responsabilités.</p>
<p>12.5.2 Contrôler et analyser les informations et les alertes de sécurité, et les diffuser au personnel compétent.</p>	<p>12.5.2 Vérifier que la responsabilité de la surveillance, de l'analyse des alertes de sécurité, et de la diffusion des informations aux chefs de division appropriés et au personnel chargé de la sécurité est formellement assignée au personnel compétent.</p>	<p>Les entités doivent également prévoir des plans de transition et/ou de succession pour le personnel clé afin d'éviter toute faille des affectations de sécurité. En effet, une telle situation peut se solder par un manque d'affectation et d'exécution des responsabilités.</p>

Conditions PCI DSS	Procédures de test	Directive
<p>12.5.3 Définir, documenter et diffuser les procédures de remontée et de réponse aux incidents liés à la sécurité pour garantir une gestion rapide et efficace de toutes les situations.</p>	<p>12.5.3 Vérifier que la responsabilité de l'établissement, de la documentation et de la distribution de la réponse aux incidents de sécurité et les procédures d'escalade est formellement assignée.</p>	
<p>12.5.4 Administrer les comptes d'utilisateur, notamment l'ajout, la suppression et la modification des comptes</p>	<p>12.5.4 Vérifier que la responsabilité de l'administration des comptes d'utilisateur (l'ajout, la suppression et la modification) et de la gestion des authentications est formellement assignée.</p>	
<p>12.5.5 Surveiller et contrôler tous les accès aux données.</p>	<p>12.5.5 Vérifier que la responsabilité de la surveillance et du contrôle de tous les accès aux données est formellement assignée.</p>	
<p>12.6 Mettre en œuvre un programme formel de sensibilisation à la sécurité pour sensibiliser tout le personnel à la politique et aux procédures de sécurité relatives aux données de titulaires de carte.</p>	<p>12.6.a Examiner le programme de sensibilisation à la sécurité pour vérifier qu'il sensibilise tout le personnel à la politique et aux procédures de sécurité relatives aux données de titulaires de carte.</p>	<p>Si le personnel n'est pas sensibilisé à ses responsabilités en matière de sécurité, les processus et les protections mis en place peuvent s'avérer inefficaces en raison des erreurs commises ou d'actes délibérés.</p>
	<p>12.6.b Examiner les procédures et la documentation du programme de sensibilisation à la sécurité, et procéder comme suit :</p>	
<p>12.6.1 Former le personnel au moment du recrutement et au moins une fois par an.</p> <p><i>Remarque : Les méthodes varient selon les postes occupés et le niveau d'accès du personnel aux données de titulaires de carte.</i></p>	<p>12.6.1.a Le programme de sensibilisation à la sécurité comprend plusieurs méthodes de sensibilisation et de formation du personnel (par exemple, affiches, lettres, mémos, formations sur le Web, réunions et promotions).</p>	<p>Si le programme de sensibilisation à la sécurité ne comporte pas de sessions annuelles de mise à niveau, les processus et procédures essentiels de sécurité pourront être oubliés ou ignorés, exposant alors des ressources stratégiques et des données de titulaires de carte.</p>
	<p>12.6.1.b Vérifier que le personnel participe aux formations de sensibilisation à la sécurité au moment de son recrutement et au moins une fois par an.</p>	
	<p>12.6.1.c Interroger un échantillon du personnel pour vérifier qu'ils ont effectué une formation de sensibilisation et qu'ils sont conscients de l'importance de la sécurité des données de titulaires de carte.</p>	

Conditions PCI DSS	Procédures de test	Directive
<p>12.6.2 Exiger que le personnel reconnaisse au moins une fois par an avoir lu et compris les procédures et la politique de sécurité.</p>	<p>12.6.2 Vérifier que le programme de sensibilisation à la sécurité exige que le personnel reconnaisse, par écrit ou par voie électronique, au moins une fois par an, avoir lu et compris la politique de sécurité des informations.</p>	<p>Exiger une reconnaissance écrite ou par voie électronique permet de s'assurer que les politiques et procédures de sécurité ont bien été lues et comprises et de l'engagement passé et futur du personnel à les respecter.</p>
<p>12.7 Effectuer une sélection préalable à l'embauche du personnel pour minimiser les risques d'attaques par des sources internes (Ces contrôles devraient inclure, par exemple, les antécédents professionnels, le casier judiciaire, les renseignements de solvabilité et la vérification des références.)</p> <p><i>Remarque : Pour le personnel dont l'embauche potentielle concerne des postes tels que celui de caissier dans un magasin, et qui n'a accès qu'à un numéro de carte à la fois à l'occasion du traitement d'une transaction, cette condition n'est qu'une recommandation.</i></p>	<p>12.7 Interroger le responsable des ressources humaines et vérifier qu'existent des contrôles des antécédents (dans les restrictions imposées par la loi) pour le personnel qui aura accès aux données de titulaires de carte ou à l'environnement de ces données.</p>	<p>La vérification approfondie des antécédents avant toute embauche de personnel amené à accéder aux données de titulaires de carte réduit le risque d'une utilisation non autorisée des PAN et autres données de titulaires de carte par des individus avec des antécédents de personnes malveillantes ou discutables.</p>
<p>12.8 Maintenir et mettre en œuvre des politiques et des procédures de gestion des prestataires de services avec lesquels les données de titulaires de carte sont partagées, ou qui pourraient affecter la sécurité des données de titulaires de carte comme suit :</p>	<p>12.8 Par le truchement d'activités d'observation, l'examen des politiques et des procédures et l'examen de la documentation connexe, vérifier que les processus sont mis en œuvre pour gérer les prestataires de services, avec lesquels les données de titulaires de carte sont partagées, ou qui pourraient affecter la sécurité des données de titulaires de carte comme suit :</p>	<p>Si un commerçant ou un prestataire de services partage des données de titulaires de carte avec un autre prestataire de services, certaines conditions s'appliquent afin de garantir que la continuité de la protection de ces données sera respectée par ces prestataires de services.</p> <p>Voici quelques types de prestataires de services : sites de stockage sur bandes de sauvegarde, prestataires de services gérés comme les sociétés d'hébergement sur le Web ou les prestataires de services de sécurité, ou encore les entités qui reçoivent des données en vue de la modélisation des fraudes, etc.</p>
<p>12.8.1 Conserver une liste des prestataires de services, y compris une description des services fournis.</p>	<p>12.8.1 Vérifier qu'une liste des prestataires de services est conservée et qu'elle comprend une description des services fournis.</p>	<p>Conserver un suivi de tous les prestataires de services permet d'identifier jusqu'où s'étendent les risques potentiels à l'extérieur de l'entreprise.</p>

Conditions PCI DSS	Procédures de test	Directive
<p>12.8.2 Maintenir un accord écrit par lequel les prestataires de services reconnaissent qu'ils sont responsables de la sécurité des données de titulaires de carte qu'ils stockent, traitent ou transmettent de la part du client, ou dans la mesure où ils pourraient avoir un impact sur la sécurité de l'environnement des données de titulaires de carte.</p> <p><i>Remarque : La formulation exacte de ce document dépendra de l'accord entre les deux parties, des détails du service fourni et des responsabilités attribuées à chaque partie. La reconnaissance n'a pas besoin d'inclure la formulation exacte précisée dans cette condition.</i></p>	<p>12.8.2 Examiner les accords écrits et confirmer qu'ils comprennent une reconnaissance par laquelle les prestataires de services admettent qu'ils sont responsables de la sécurité des données de titulaires de carte qu'ils stockent, traitent ou transmettent de la part du client, ou dans la mesure où ils pourraient avoir un impact sur la sécurité de l'environnement des données de titulaires de carte.</p>	<p>Par cet accord, les prestataires de services reconnaissent leur engagement à assurer la sécurité appropriée des données de titulaires de carte obtenues auprès de leurs clients. Le niveau de responsabilité des prestataires de services concernant la sécurité des données de titulaires de carte dépendra du service concerné et de l'accord entre le prestataire et l'entité évaluée.</p> <p>En conjonction avec la condition 12.9, cette condition consiste à promouvoir un niveau d'entente constant entre les parties concernant les responsabilités qui leur incombent dans le cadre de la norme PCI DSS. Par exemple, l'accord peut inclure les conditions applicables de la norme PCI DSS à maintenir dans le cadre de la prestation de service.</p>
<p>12.8.3 S'assurer que le processus de sélection des prestataires de services est bien défini, et qu'il inclut notamment des contrôles préalables à l'engagement.</p>	<p>12.8.3 Vérifier que les politiques et les procédures sont documentées et mises en œuvre, notamment le contrôle préalable à l'engagement de tout prestataire de services.</p>	<p>Ce processus garantit que le choix du prestataire de services a été vérifié en interne par l'organisation, et doit comporter une analyse des risques avant d'établir une relation formelle quelconque avec ce prestataire.</p> <p>Les processus et les objectifs de diligence spécifique seront différents pour chaque organisation. Les exemples de considération peuvent inclure les pratiques de rapport du prestataire, les procédures de notification d'infraction et de réponse aux incidents, les détails de la manière avec laquelle les responsabilités de la norme PCI DSS sont affectées entre chaque partie, comment le prestataire valide sa conformité à la norme PCI DSS et quelles preuves il peut fournir, etc.</p>

Conditions PCI DSS	Procédures de test	Directive
<p>12.8.4 Maintenir un programme qui contrôle la conformité des prestataires de services à la norme PCI DSS au moins une fois par an.</p> <p>12.8.5 Maintenir les informations concernant les conditions de la norme PCI DSS qui sont gérées par chaque prestataire de service et celles qui sont gérées par l'organisation.</p>	<p>12.8.4 Vérifier que l'entité a mis en place un programme qui contrôle la conformité de ses prestataires de services à la norme PCI DSS au moins une fois par an.</p> <p>12.8.5 Vérifier que l'organisation conserve les informations concernant les conditions de la norme PCI DSS qui sont gérées par chaque prestataire de service et celles qui sont gérées par l'organisation.</p>	<p>Connaître le statut du prestataire de services en termes de conformité à la norme PCI DSS permet de s'assurer et de tenir compte du fait qu'il doit respecter les mêmes conditions que votre organisation. Si le prestataire de services offre des services divers, cette condition doit s'appliquer aux services réellement fournis au client et aux services qui sont dans le champ d'application de l'évaluation PCI DSS du client.</p> <p>Les informations conservées par une entité dépendront de l'accord passé avec leurs prestataires, le type de service, etc. Le but visé est que l'entité évaluée comprenne les conditions de la norme PCI DSS que ses prestataires ont convenu de respecter.</p>
<p>12.9 Condition supplémentaire pour les prestataires de services uniquement : Les prestataires de services reconnaissent par écrit qu'ils sont responsables de la sécurité des données de titulaires de carte qu'ils stockent, traitent ou transmettent de la part du client, ou dans la mesure où ils pourraient avoir un impact sur la sécurité de l'environnement des données de titulaires de carte.</p> <p><i>Remarque : La formulation exacte de ce document dépendra de l'accord entre les deux parties, des détails du service fourni et des responsabilités attribuées à chaque partie. La reconnaissance n'a pas besoin d'inclure la formulation exacte précisée dans cette condition.</i></p>	<p>12.9 Procédure de tests supplémentaires pour évaluer les prestataires de services uniquement : Examiner les politiques et les procédures du prestataire de service et observer les modèles utilisés pour les accords écrits afin de confirmer que le prestataire de service reconnaît par écrit aux clients qu'il respectera toutes les conditions applicables de la norme PCI DSS dans la mesure où il dispose ou stocke, traite ou transmet les données de titulaires de carte au nom du client ou dans la mesure où elles peuvent influencer sur la sécurité de l'environnement de données de titulaires de carte du client.</p>	<p><i>Remarque : Cette condition ne s'applique que lorsque l'entité évaluée est un prestataire de services.</i></p> <p>En conjonction avec la condition 12.8.2, cette condition est destinée à promouvoir un niveau de compréhension constant entre les prestataires de services et leurs clients, concernant les responsabilités applicables de la norme PCI DSS. Par cet accord, les prestataires de services reconnaissent leur engagement à assurer la sécurité appropriée des données de titulaires de carte obtenues auprès de leurs clients.</p> <p>Les politiques et les procédures internes du prestataire de services concernant son engagement auprès des clients, ainsi que les modèles utilisés pour les accords écrits, doivent prévoir une disposition pour la reconnaissance de la norme PCI DSS. La méthode par laquelle le prestataire de service peut effectuer cette reconnaissance par écrit doit être convenue entre le prestataire et ses clients.</p>

Conditions PCI DSS	Procédures de test	Directive
<p>12.10 Mettre en œuvre un plan de réponse aux incidents. Être prêt à réagir immédiatement à toute intrusion dans le système.</p>	<p>12.10 Examiner le plan de réponse aux incidents et les procédures connexes pour vérifier que l'organisation est prête à répondre immédiatement à une faille du système, comme suit :</p>	<p>Sans un plan détaillé de réponse aux incidents, correctement diffusé, lu et compris par les parties responsables, une certaine confusion et l'absence de réponses unifiées pourraient entraîner une interruption des activités de l'entreprise, avec une publicité inutile de la part des médias publics, ainsi que de nouvelles responsabilités légales.</p>
<p>12.10.1 Élaborer le plan de réponse aux incidents à mettre en place en cas d'intrusion dans le système. S'assurer que le plan prévoit au moins les points suivants :</p> <ul style="list-style-type: none"> • Rôles, responsabilités et stratégies de communication et de contact en cas d'incident, notamment notification des marques de cartes de paiement, au minimum ; • Les procédures de réponse aux incidents spécifiques ; • Les procédures de continuité et de reprise des affaires ; • Processus de sauvegarde des données ; • Analyse des exigences légales en matière de signalement des incidents ; • Couverture et réponses de tous les composants stratégiques du système ; • Référence ou inclusion des procédures de réponse aux incidents des marques de cartes de paiement. 	<p>12.10.1.a Vérifier que le plan de réponse aux incidents inclut :</p> <ul style="list-style-type: none"> • Les rôles, les responsabilités et les stratégies de communication en cas d'incident, notamment la notification des marques de cartes de paiement, au minimum ; • Les procédures de réponse aux incidents spécifiques ; • Les procédures de continuité et de reprise des affaires ; • Processus de sauvegarde des données ; • L'analyse des exigences légales en matière de signalement des incidents (par exemple, le California Bill 1386, qui exige la notification des consommateurs affectés en cas d'incident avéré ou soupçonné pour toute entreprise comptant des résidents en Californie dans sa base de données) ; • La couverture et les réponses de tous les composants stratégiques du système ; • Référence ou inclusion des procédures de réponse aux incidents des marques de cartes de paiement. <p>12.10.1.b Interroger le personnel et examiner la documentation d'un incident ou d'une alerte signalés antérieurement afin de vérifier que les procédures et le plan documenté de réponse aux incidents sont suivis.</p>	<p>Le plan de réponse aux incidents doit être complet et comporter tous les éléments essentiels permettant à la société de réagir efficacement en cas de violation susceptible d'affecter les données de titulaires de carte.</p>

Conditions PCI DSS	Procédures de test	Directive
<p>12.10.2 Examiner et tester le plan au moins une fois par an, y compris les éléments répertoriés dans la condition 12.10.1.</p>	<p>12.10.2 Interroger le personnel et examiner la documentation sur les tests pour vérifier que le plan est testé au moins une fois par an et que ces tests comprennent tous les éléments répertoriés dans la condition 12.10.1.</p>	<p>Sans des tests appropriés, des étapes essentielles peuvent être omises et entraîner une exposition accrue durant un incident.</p>
<p>12.10.3 Désigner le personnel spécifique disponible 24 heures sur 24 et sept jours sur sept pour répondre aux alertes.</p>	<p>12.10.3 À travers l'observation, l'examen des politiques et les contacts avec le personnel responsable, vérifier que le personnel désigné est disponible 24 heures sur 24 et sept jours sur sept pour répondre aux incidents et que toutes les activités non autorisées, la détection des points d'accès sans-fil non autorisés, les alertes des systèmes de détection d'incidents et/ou le signalement de toute modification non autorisée du contenu des fichiers ou des systèmes stratégiques sont sous surveillance.</p>	<p>Sans une équipe de réponse aux incidents bien formée et disponible à tout moment, le réseau peut être gravement endommagé, et les données et les systèmes stratégiques peuvent être « pollués » par une manipulation inappropriée des systèmes ciblés. Cela peut empêcher l'enquête réalisée après un incident d'aboutir.</p>
<p>12.10.4 Organiser la formation appropriée du personnel en charge de la réponse aux violations de la sécurité.</p>	<p>12.10.4 Vérifier par l'observation, l'examen des politiques et les contacts avec le personnel responsable que le personnel chargé de la réponse aux violations de la sécurité reçoit une formation périodique.</p>	
<p>12.10.5 Inclure les alertes des systèmes de surveillance de sécurité, notamment les systèmes d'intrusion-détection, intrusion-prévention, les pare-feu et les systèmes de surveillance de l'intégrité des fichiers.</p>	<p>12.10.5 Suite à l'observation et à l'examen des processus, vérifier que le contrôle et la réponse aux alertes émises par les systèmes de contrôle de sécurité sont couverts dans le plan de réponse aux incidents.</p>	<p>Ces systèmes de surveillance, axés sur les risques potentiels encourus par les données, sont essentiels pour agir rapidement afin de prévenir une violation et ils doivent être intégrés aux processus de réponse aux incidents.</p>
<p>12.10.6 Définir un processus de modification et de développement du plan de réponse aux incidents en fonction des leçons apprises, et tenir compte de l'évolution du secteur.</p>	<p>12.10.6 À travers l'observation, l'examen des politiques et les contacts avec le personnel, vérifier qu'un processus est en place pour la modification et le développement du plan de réponse aux incidents en fonction des leçons apprises et la prise en compte de l'évolution du secteur.</p>	<p>Intégrer au plan de réponse aux incidents les « leçons tirées » après un problème permet de garder ce plan à jour et de réagir face aux nouvelles menaces et tendances en matière de sécurité.</p>

Conditions PCI DSS	Procédures de test	Directive
<p>12.11 Condition supplémentaire pour les prestataires de services uniquement : Effectuer des vérifications au moins une fois par trimestre pour confirmer que le personnel respecte les politiques de sécurité et les procédures opérationnelles. Les examens doivent couvrir les processus suivants :</p> <ul style="list-style-type: none"> • Examens quotidiens des journaux • Examens des règles liées aux pare-feu • Application des normes de configuration aux nouveaux systèmes • Intervention suite aux alertes de sécurité • Modifier les processus de gestion <p><i>Remarque : Cette condition est considérée comme une meilleure pratique jusqu'au 31 janvier 2018, après quoi ce sera une obligation.</i></p>	<p>12.11.a Examiner les politiques et les procédures pour vérifier que les processus sont définis en vue de vérifier et de confirmer que le personnel respecte les politiques de sécurité et les procédures opérationnelles, et que les examens couvrent ce qui suit :</p> <ul style="list-style-type: none"> • Examens quotidiens des journaux • Examens des règles liées aux pare-feu • Application des normes de configuration aux nouveaux systèmes • Intervention suite aux alertes de sécurité • Modifier les processus de gestion <p>12.11.b Interroger le personnel responsable et examiner les registres des examens pour vérifier que ces derniers sont effectués au moins une fois par trimestre.</p>	<p>Remarque : Cette condition ne s'applique que lorsque l'entité évaluée est un prestataire de services.</p> <p>Une confirmation régulière du suivi des politiques et des procédures de sécurité permet de garantir que les contrôles prévus sont actifs et fonctionnent comme prévu. Il ne s'agit pas d'exécuter d'autres conditions PCI DSS mais de confirmer que les procédures sont suivies comme il se doit.</p>
<p>12.11.1 Condition supplémentaire pour les prestataires de services uniquement : La gestion de la documentation du processus d'examens trimestriels comprend ce qui suit :</p> <ul style="list-style-type: none"> • Documentation des résultats d'examens • Examiner et valider les résultats par le personnel responsable du programme de conformité à la norme PCI DSS <p><i>Remarque : Cette condition est considérée comme une meilleure pratique jusqu'au 31 janvier 2018, après quoi ce sera une obligation.</i></p>	<p>12.11.1 Examiner la documentation des examens trimestriels pour vérifier ce qui suit :</p> <ul style="list-style-type: none"> • Documentation des résultats d'examens • Examiner et valider les résultats par le personnel responsable du programme de conformité à la norme PCI DSS 	<p>Remarque : Cette condition ne s'applique que lorsque l'entité évaluée est un prestataire de services.</p> <p>Ces vérifications indépendantes visent à confirmer si les activités de sécurité sont effectuées régulièrement. Ces examens peuvent également être utilisés pour vérifier que des preuves suffisantes sont maintenues, par exemple, des journaux d'audit, des rapports d'analyse de vulnérabilité, des examens de pare-feu, etc. afin d'aider l'entité à se préparer pour sa prochaine évaluation de conformité à la norme PCI DSS.</p>

Annexe A : Autres conditions de la norme PCI DSS

Cette annexe comprend d'autres conditions de la norme PCI DSS pour différents types d'entités. Les sections dans cette annexe comprennent :

- Annexe A1 : Autres conditions de la norme PCI DSS s'appliquant aux prestataires de services d'hébergement partagé
- Annexe A2 : Autres conditions de la norme PCI DSS s'appliquant aux entités qui utilisent le SSL/TLS initial
- Annexe A3 : Validation complémentaire des entités désignées

Des directives et des informations d'applicabilité sont fournies dans chaque section.

Annexe A1 : Autres conditions de la norme PCI DSS s'appliquant aux fournisseurs d'hébergement partagé

Comme il est indiqué dans les conditions 12.8 et 12.9, tous les prestataires de services qui ont accès aux données de titulaires de carte (notamment les prestataires de services d'hébergement partagé) doivent respecter la norme PCI DSS. En outre, la condition 2.6 stipule que les prestataires de services d'hébergement partagé doivent protéger les données et l'environnement hébergés de chaque entité. En conséquence, les prestataires de services d'hébergement partagé doivent par ailleurs se conformer aux exigences définies dans cette annexe.

Conditions A1	Procédures de test	Directive
<p>A1 Protéger les données et l'environnement hébergés de chaque entité (c'est-à-dire le commerçant, le prestataire de services ou toute autre entité) conformément aux conditions A1.1 à A1.4 :</p> <p>Un prestataire de services d'hébergement doit satisfaire à ces conditions ainsi qu'aux conditions de toutes les autres rubriques pertinentes de la norme PCI DSS.</p> <p><i>Remarque : Même si un prestataire de services d'hébergement peut satisfaire à ces conditions, la conformité de l'entité qui a recours au prestataire de services d'hébergement n'est pas garantie. Chaque entité doit se conformer à la norme PCI DSS et doit valider cette conformité comme applicable.</i></p>	<p>A1 Dans le cadre spécifique de l'évaluation d'un prestataire de services d'hébergement partagé au regard de la norme PCI DSS, afin de vérifier que les prestataires de services d'hébergement protègent les données et l'environnement hébergés des entités (commerçants et prestataires de services), sélectionner un échantillon de serveurs (Microsoft Windows et Unix/Linux) appartenant à quelques commerçants et prestataires de services hébergés représentatifs et exécuter les conditions A1.1 à A1.4 décrits ci-dessous :</p>	<p>L'annexe A de la norme PCI DSS est destinée aux prestataires de services d'hébergement partagé qui souhaitent fournir à leurs clients commerçants et/ou prestataires de services un environnement d'hébergement conforme à cette norme.</p>

Conditions A1	Procédures de test	Directive
<p>A1.1 S'assurer que chaque entité ne met en œuvre que les processus qui ont accès à l'environnement des données de titulaires de carte qui la concerne.</p>	<p>A1.1 Si un prestataire de services d'hébergement partagé autorise des entités (par exemple, commerçants ou prestataires de services) à déployer leurs propres applications, vérifier que ces processus d'application sont exécutés avec l'ID unique de l'entité. Par exemple :</p> <ul style="list-style-type: none"> • Aucune entité sur le système ne peut utiliser un ID d'utilisateur partagé sur le serveur Web. • Tous les scripts CGI utilisés par une entité doivent être créés et exécutés sous l'ID d'utilisateur unique de l'entité. 	<p>Si un commerçant ou un prestataire de services est autorisé à exécuter ses propres applications sur le serveur partagé, il doit le faire avec l'ID utilisateur du commerçant ou du prestataire de services, et non en tant qu'utilisateur privilégié.</p>
<p>A1.2 Restreindre l'accès et les privilèges de chaque entité à son propre environnement de données de titulaires de carte.</p>	<p>A1.2.a Vérifier que l'ID d'utilisateur de tout processus d'application n'est pas un utilisateur avec des privilèges (racine/admin).</p> <p>A1.2.b Vérifier que chaque entité (commerçant, prestataire de services) a des autorisations de lecture, d'écriture ou d'exécution uniquement sur les fichiers et les répertoires qui lui appartiennent ou sur les fichiers système nécessaires (autorisations restreintes au moyen d'autorisations sur le système de fichiers, de listes de contrôle d'accès, chroot, jailshell, etc.).</p> <p>Important : Les fichiers d'une entité ne peuvent pas être partagés par groupe.</p> <p>A1.2.c Vérifier que les utilisateurs d'une entité n'ont pas un accès en écriture aux fichiers binaires d'un système partagé.</p> <p>A1.2.d Vérifier que l'affichage des entrées des journaux est limité à l'entité propriétaire de ces journaux.</p> <p>A1.2.e Pour s'assurer que chaque entité ne puisse pas monopoliser des ressources serveur en vue d'exploiter des vulnérabilités (notamment, erreur, concurrence critique et conditions de reprise entraînant, par exemple, la saturation de la mémoire tampon), vérifier que des restrictions sont en place pour l'usage de ces ressources système :</p> <ul style="list-style-type: none"> • Espace disque, • Bande passante, • Mémoire, • Processeur 	<p>Pour s'assurer que l'accès et les privilèges sont restreints de telle sorte que chaque commerçant et prestataire de services ne puisse accéder qu'à son propre environnement, tenir compte des facteurs suivants :</p> <ol style="list-style-type: none"> 1. Privilèges de l'ID utilisateur de serveur Web du prestataire de service ou du commerçant ; 2. Permissions accordées pour lire, écrire et exécuter des fichiers ; 3. Permissions accordées pour écrire les systèmes binaires ; 4. Permissions accordées aux fichiers de journalisation de prestataire de service et de commerçant ; et 5. Contrôles pour assurer qu'un commerçant ou un prestataire de service ne puisse pas monopoliser les ressources du système.

Conditions A1	Procédures de test	Directive
<p>A1.3 S'assurer que la journalisation et les vérifications à rebours sont activées, uniques à l'environnement des données de titulaires de carte de chaque entité et conformes à la condition 10 de la norme PCI DSS.</p>	<p>A1.3 Vérifier que le prestataire de services d'hébergement partagé a activé la journalisation comme suit, pour l'environnement de chaque commerçant et prestataire de services :</p> <ul style="list-style-type: none"> • Les journaux sont activés pour les applications tierces courantes ; • Les journaux sont activés par défaut ; • Les journaux peuvent être consultés par l'entité à laquelle ils appartiennent ; • Les emplacements des journaux sont clairement communiqués à l'entité propriétaire. 	<p>Dans un environnement d'hébergement partagé, des journaux doivent être disponibles afin que les commerçants et les prestataires de services puissent accéder et examiner les journaux spécifiques à leur environnement de données de titulaires de carte.</p>
<p>A1.4 Activer les processus d'investigation informatique légale rapide en cas d'incident dans l'environnement d'un commerçant ou d'un prestataire de services.</p>	<p>A1.4 Vérifier que le prestataire de services d'hébergement partagé a des politiques écrites garantissant la mise en œuvre rapide d'investigations informatiques légales sur les serveurs en cas d'incident.</p>	<p>Les fournisseurs d'hébergement partagé doivent disposer de processus permettant une réponse rapide et simple en cas d'enquête légale après incident, et permettant un niveau de détail approprié, allant jusqu'à comprendre les informations sur le commerçant ou le prestataire de services à titre individuel.</p>

Annexe A2 : Autres conditions de la norme PCI DSS s'appliquant aux entités qui utilisent le SSL/TLS initial

Les entités, qui utilisent le SSL et le TLS initial, doivent s'employer à adopter un protocole cryptographique fiable dès que possible. Qui plus est, le SSL et/ou le TLS initial ne doivent pas être introduits dans des environnements contenant déjà ces protocoles. Au moment de la publication, les vulnérabilités connues sont difficiles à exploiter dans les environnements de paiement POS POI. Cependant, de nouvelles vulnérabilités pourraient survenir à tout moment. C'est à l'organisation de s'informer des dernières tendances en matière de vulnérabilité et de déterminer si celles-ci sont susceptibles de créer des failles connues.

Les conditions de la norme PCI DSS directement concernées sont les suivantes :

- Condition 2.2.3** Implémentation des fonctions de sécurité supplémentaires pour tout service, protocole ou démon nécessaire et jugé comme non sécurisé.
- Condition 2.3** Crypter tous les accès administratifs non console, à l'aide d'une cryptographie robuste.
- Condition 4.1** Utiliser des protocoles de cryptographie et de sécurité robustes pour sauvegarder les données des titulaires de cartes sensibles lors de leur transmission sur des réseaux publics et ouverts.

Ne pas utiliser le SSL et le TLS initial en tant que contrôles de sécurité pour remplir ces conditions. Les mesures suivantes sont disponibles pour aider les entités à abandonner le SSL et le TLS initial :

- Les nouvelles implémentations ne doivent pas utiliser le SSL ou le TLS initial comme contrôles de sécurité.
- D'ici le 30 juin **2016**, **tous les prestataires de services doivent proposer un service sécurisé.**
- Après le 30 juin **2018**, toutes les entités doivent avoir interrompu leurs recours au SSL/TLS initial en tant que contrôles de sécurité et utiliser exclusivement les versions sécurisées du protocole (le recours à certains terminaux POS POI est autorisé et décrit dans le dernier point ci-dessous).
- D'ici le 30 juin 2018, les implémentations existantes, qui utilisent le SSL et/ou le TLS initial, doivent comporter un plan formel d'atténuation des risques et de migration.
- Vous pouvez continuer d'utiliser les terminaux POS POI (et les points de terminaisons SSL/TLS auxquels ils sont connectés) en tant que contrôles de sécurité après le 30 juin 2018 après vous être assuré qu'ils ne sont pas susceptibles d'occasionner des failles connues pour le SSL ou le TLS initial.

Cette annexe s'applique à toutes les entités ayant recours au SSL/TLS initial en tant que contrôles de sécurité pour protéger le CDE et/ou le CHD (par exemple, utilisation du SSL/TLS initial pour remplir la condition 2.2.3, 2.3 ou 4.1 de la PCI DSS). Se reporter aux *récentes informations complémentaires PCI SSC sur la migration depuis le SSL et le TLS initial* pour obtenir des directives complémentaires sur l'utilisation du SSL/TLS initial.

Conditions A2	Procédures de test	Directive
<p>A2.1 Lorsque les terminaux POS POI (et les points de terminaison SSL/TLS auxquels se connecter) utilisent le SSL et/ou le TLS initial, l'entité doit :</p> <ul style="list-style-type: none"> • Confirmer les dispositifs qui n'ont pas de failles connues pour ces protocoles. <p>Ou :</p> <ul style="list-style-type: none"> • Disposer d'un plan formel d'atténuation des risques et de migration. 	<p>A2.1 Pour les terminaux POS POI (et les points de terminaison SSL/TLS auxquels se connecter) qui utilisent le SSL et/ou le TLS initial :</p> <ul style="list-style-type: none"> • Confirmer que l'entité dispose de la documentation (par exemple, la documentation des fournisseurs, les détails de configuration système/réseau, etc.) qui vérifie que les dispositifs n'ont pas de failles connues pour le SSL/TLS initial. <p><i>Ou :</i></p> <ul style="list-style-type: none"> • Remplir la condition A2.2 ci-dessous. 	<p>Le POI peut continuer avec le SSL/TLS initial si la preuve est avancée que le POI n'a pas de failles actuellement connues. Cependant, le SSL est une technologie désuète, qui peut faire l'objet d'autres vulnérabilités en matière de sécurité à l'avenir. Il est donc vivement recommandé de mettre à niveau les environnements POI vers un protocole sécurisé, dès que possible. Si le SSL/TLS initial n'est pas requis dans l'environnement, le recours et le repli relatifs à ces versions doivent être désactivés.</p> <p>Si l'environnement POS POI a des failles connues, envisager une migration vers un autre protocole sécurisé immédiatement.</p> <p>Remarque : Le recours autorisé aux POS POI sans failles actuellement connues repose sur des risques actuels et connus. Si de nouvelles failles sont introduites et que les environnements POI ne sont pas protégés, une mise à niveau est indispensable.</p>
<p>A2.2 Les entités dotées d'implémentations existantes (autres que celles autorisées dans la condition A2.1) et utilisant le SSL et/ou TLS initial doivent disposer d'un plan formel d'atténuation des risques et de migration.</p>	<p>A2.2 Examiner la documentation sur le plan d'atténuation des risques et de migration pour vérifier ce qui suit :</p> <ul style="list-style-type: none"> • Description de l'utilisation, y compris : le type de données transmises, les types et le nombre de systèmes qui utilisent et/ou soutiennent le SSL/TLS initial, le type d'environnement ; • Les résultats d'évaluation des risques et les contrôles d'atténuation des risques en vigueur ; • Description des processus pour contrôler les nouvelles vulnérabilités associées au SSL/TLS initial ; • Description des processus liés au contrôle de changement et implémentés pour s'assurer que le SSL/TLS initial n'est pas implémenté dans les nouveaux environnements ; • Aperçu du plan de migration, y compris la date d'achèvement cible fixée au 30 juin 2018 au plus tard. 	<p>Le plan formel d'atténuation des risques et de migration est un document préparé par l'entité qui détaille les projets de migration vers un protocole sécurisé, et décrit les contrôles de l'entité pour atténuer le risque associé au SSL/TLS initial tant que la migration n'est pas terminée.</p> <p>Se reporter aux récentes informations complémentaires PCI SSC sur la migration depuis le SSL et le TLS initial pour obtenir des directives complémentaires sur les plans d'atténuation des risques et de migration.</p>

Conditions A2	Procédures de test	Directive
<p>A2.3 Condition supplémentaire pour les prestataires de services uniquement : D'ici le 30 juin 2016, tous les prestataires de services doivent proposer un service sécurisé.</p> <p>Remarque : D'ici le 30 juin 2016, le prestataire de services doit proposer soit un protocole sécurisé compris dans son offre de services soit un plan documenté d'atténuation des risques et de migration (conformément à la condition A2.2) avec une date cible pour offrir un protocole sécurisé d'ici le 30 juin 2016. Après cette date, tous les prestataires de services doivent offrir un protocole sécurisé pour leurs services.</p>	<p>A2.3 Examiner les configurations système et la documentation connexe pour vérifier que le prestataire de services offre un protocole sécurisé pour ses services.</p>	<p>Se reporter aux « Prestataires de services » dans le <i>Glossaire des termes, abréviations et acronymes PCI DSS et PA-DSS</i> pour obtenir d'autres détails.</p>

Annexe A3 : Validation complémentaire des entités désignées (DESV)

Cette annexe s'applique uniquement aux entités désignées par des marques de paiement ou un acquéreur dans la mesure où une validation supplémentaire des conditions PCI DSS existantes est exigée. Exemples d'entités auxquelles cette annexe **peut** s'appliquer :

- Entités avec de grands volumes de stockage, traitement et/ou transmission des données de titulaires de carte,
- Entités avec des points d'agrégation pour les données de titulaires de carte, ou
- Entités ayant subi des fuites importantes ou répétées des données de titulaires de cartes.

Ces étapes de validation complémentaire permettent d'améliorer la gestion efficace et continue des contrôles PCI DSS grâce à la validation des processus d'affaires courantes (business-as-usual, BAU), une validation accrue et une réflexion sur la détermination du champ d'application.

Les étapes de validation supplémentaires figurant dans ce document sont classées en fonction des domaines de contrôle suivants :

- A3.1** *Implémenter un programme de conformité à la norme PCI DSS.*
- A3.2** *Documenter et valider le champ d'application de la norme PCI DSS.*
- A3.3** *Confirmer que la norme PCI DSS est incorporée dans les activités courantes (BAU).*
- A3.4** *Contrôler et gérer l'accès logique à l'environnement des données de titulaires de carte.*
- A3.5** *Identifier et résoudre les événements suspects.*

Remarque : *Certaines conditions comportent des critères temporels (par exemple, au moins une fois par trimestre ou semestre) afin d'exécuter certaines activités dans les délais spécifiés. Dans l'évaluation initiale de ce document, une activité ne doit pas être effectuée en fonction de tous ces délais pendant l'année précédente si l'évaluateur vérifie ce qui suit :*

- 1) *L'activité a été exécutée conformément à la condition applicable dans le délai le plus récent (c'est-à-dire, le dernier trimestre ou semestre), et*
- 2) *L'entité possède des politiques et des procédures documentées pour poursuivre l'activité dans les délais impartis.*

Pour les années à venir après l'évaluation initiale, une activité doit être réalisée dans chaque délai prescrit (par exemple, une activité trimestrielle doit avoir eu lieu pour chacun des quatre trimestres de l'année précédente).

Remarque : *Une entité doit faire l'objet d'une évaluation conformément à cette annexe **UNIQUEMENT** si un acquéreur ou une marque de paiement l'exige ainsi.*

Conditions A3	Procédures de test	Directive
A3.1 Implémenter un programme de conformité à la norme PCI DSS		
<p>A3.1.1 L'équipe de direction doit définir la responsabilité relative à la protection des données de titulaires de carte et un programme de conformité à la norme PCI DSS, comme suit :</p> <ul style="list-style-type: none"> • Responsabilité globale pour respecter la conformité à la norme PCI DSS • Définition d'une charte pour un programme de conformité à la norme PCI DSS • Envoi de mises à jour à l'équipe de direction et au conseil d'administration sur les initiatives et les problèmes relatifs à la conformité à la norme PCI DSS, y compris les mesures de résolution, au moins une fois par an <p>Référence de la norme PCI DSS : <i>Condition 12</i></p>	<p>A3.1.1.a Examiner la documentation pour vérifier que l'équipe de direction a affecté une responsabilité globale relative au respect de la conformité à la norme PCI DSS de l'entité.</p> <p>A3.1.1.b Examiner la charte PCI DSS de la société pour vérifier si elle décrit les conditions propres au programme de conformité à la norme PCI DSS.</p> <p>A3.1.1.c Examiner les procès-verbaux et/ou les présentations des réunions de l'équipe de direction et du conseil d'administration pour assurer une communication annuelle (au minimum) des initiatives et des résolutions relatives à la conformité à la norme PCI DSS.</p>	<p>L'affectation de responsabilités relatives à la conformité à la norme PCI DSS par l'équipe de direction assure une visibilité optimale du programme de conformité à la norme PCI DSS et permet de poser les questions pertinentes pour déterminer l'efficacité du programme et influencer les priorités stratégiques. La responsabilité globale du programme de conformité à la norme PCI DSS peut être affectée à des rôles individuels et/ou aux divisions au sein de l'organisation.</p>
<p>A3.1.2 Un programme formel de conformité à la norme PCI DSS doit exister et inclure ce qui suit :</p> <ul style="list-style-type: none"> • Définition des activités pour gérer et contrôler les activités de conformité à la norme PCI DSS, y compris les affaires courantes • Processus d'évaluation annuelle de la norme PCI DSS • Processus relatifs à la validation continue des conditions de la norme PCI DSS (par exemple, journalière, hebdomadaire, trimestrielle, etc. conformément à la condition) • Processus pour analyser les impacts sur 	<p>A3.1.2.a Examiner les politiques et les procédures relatives à la sécurité des informations pour vérifier que les processus sont définis spécifiquement pour les points suivants :</p> <ul style="list-style-type: none"> • Gestion et contrôle de la conformité globale à la norme PCI DSS, y compris les affaires courantes • Évaluation(s) annuelle(s) de la norme PCI DSS • Validation continue des conditions de la norme PCI DSS • Analyse des impacts sur les affaires de la société afin de déterminer les incidences éventuelles de la norme PCI DSS dans le cadre des décisions commerciales stratégiques 	<p>Un programme formel de conformité permet à une organisation de contrôler la fiabilité de ses contrôles de sécurité, d'être proactive en cas de contrôle défaillant et de communiquer efficacement sur ses activités et l'état de conformité au sein de l'organisation.</p> <p>Le programme de conformité à la norme PCI DSS peut être un programme dédié ou faire partie d'un programme global de conformité et/ou de gouvernance. Il doit inclure une méthodologie bien définie qui illustre une évaluation cohérente et efficace. Exemples de méthodologies : Cercle Deming axé sur quatre étapes : Planifier - Faire - Vérifier - Agir (PFVA), ISO 27001, COBIT, DMAIC et Six Sigma.</p>

Conditions A3	Procédures de test	Directive
<p>les affaires de la société afin de déterminer les incidences éventuelles de la norme PCI DSS dans le cadre des décisions commerciales stratégiques</p> <p>Référence de la norme PCI DSS : Conditions 1-12</p>		<p>(suite à la page suivante)</p>
	<p>A3.1.2.b Interroger le personnel et observer les activités de conformité pour vérifier que les processus définis sont implémentés comme suit :</p> <ul style="list-style-type: none"> • Gestion et contrôle de la conformité globale à la norme PCI DSS, y compris les affaires courantes • Évaluation(s) annuelle(s) de la norme PCI DSS • Validation continue des conditions de la norme PCI DSS • Analyse des impacts sur les affaires de la société afin de déterminer les incidences éventuelles de la norme PCI DSS dans le cadre des décisions commerciales stratégiques 	<p>La gestion et le contrôle du programme global de conformité à la norme PCI DSS au sein d'une organisation comprennent l'identification d'activités à effectuer sur une base quotidienne, hebdomadaire, mensuelle, trimestrielle ou annuelle. Il est essentiel de vérifier que ces activités sont exécutées conformément à ces facteurs temporels (par exemple, en utilisant une auto-évaluation de sécurité ou une méthodologie PFVA).</p> <p>Parmi les exemples de décisions commerciales stratégiques à analyser pour déterminer les impacts éventuels de la norme PCI DSS, on peut inclure les fusions et les acquisitions, les achats de nouvelles technologies ou les nouveaux canaux d'acceptation de paiement.</p>
<p>A3.1.3 Les rôles et les responsabilités liés à la conformité à la norme PCI DSS doivent être spécifiquement définis et affectés formellement à un ou plusieurs membres du personnel, y compris ce qui suit :</p> <ul style="list-style-type: none"> • Gestion des activités courantes relatives à la norme PCI DSS • Gestion des évaluations annuelles relatives à la norme PCI DSS • Gestion de la validation continue des conditions de la norme PCI DSS (par exemple, journalière, hebdomadaire, trimestrielle, etc. conformément à la condition) 	<p>A3.1.3.a Examiner les politiques et les procédures de sécurité des informations et interroger le personnel pour vérifier que les rôles et les responsabilités sont clairement définis et que les obligations sont affectées pour inclure ce qui suit :</p> <ul style="list-style-type: none"> • Gestion des activités courantes relatives à la norme PCI DSS • Gestion des évaluations annuelles relatives à la norme PCI DSS • Gestion de la validation continue des conditions de la norme PCI DSS (par exemple, journalière, hebdomadaire, trimestrielle, etc. conformément à la condition) • Gestion de l'analyse des impacts sur les affaires 	<p>La définition formelle des rôles et des responsabilités relatifs à la conformité à la norme PCI DSS permet d'assurer la responsabilisation et le contrôle des efforts continus pour garantir la conformité à la norme PCI DSS. Ces rôles peuvent être affectés à un ou plusieurs propriétaires dans des domaines différents. La propriété doit être affectée à des individus autorisés à prendre des décisions en fonction des risques et nommés responsables pour les fonctions concernées. Les obligations doivent être définies formellement et les propriétaires doivent cerner leurs responsabilités et les attentes à leur égard.</p>

Conditions A3	Procédures de test	Directive
<ul style="list-style-type: none"> Gestion de l'analyse des impacts sur les affaires de la société afin de déterminer les incidences éventuelles de la norme PCI DSS dans le cadre des décisions commerciales stratégiques <p>Référence de la norme PCI DSS : Condition 12</p>	<p>de la société afin de déterminer les incidences éventuelles de la norme PCI DSS dans le cadre des décisions commerciales stratégiques</p> <p>A3.1.3.b Interroger les membres du personnel et vérifier qu'ils se sont familiarisés avec les responsabilités de conformité à la norme PCI DSS.</p>	

Conditions A3	Procédures de test	Directive
<p>A3.1.4 Fournir une formation actualisée sur la norme PCI DSS et la sécurité des informations au moins une fois par an au personnel chargé d'assurer la conformité à la norme PCI DSS (comme indiqué dans A3.1.3).</p> <p>Référence de la norme PCI DSS : Condition 12</p>	<p>A3.1.4.a Examiner les politiques et les procédures relatives à la sécurité des informations pour vérifier qu'une formation sur la norme PCI DSS et la sécurité des informations est requise au moins une fois par an pour chaque rôle chargé d'assurer la conformité à la norme PCI DSS.</p> <p>A3.1.4.b Interroger le personnel et examiner les certificats de participation ou autres registres pour vérifier que le personnel chargé d'assurer la conformité à la norme PCI DSS reçoit une formation actualisée sur la norme PCI DSS et/ou la sécurité des informations au moins une fois par an.</p>	<p>Le personnel chargé d'assurer la conformité à la norme PCI DSS a des besoins de formation spécifiques qui dépassent typiquement le contenu couvert par la formation générale de sensibilisation à la sécurité. Les individus chargés d'assurer la conformité à la norme PCI DSS doivent recevoir une formation spécialisée qui, outre la sensibilisation générale à la sécurité des informations, met l'accent sur des sujets, des compétences, des processus ou des méthodologies de sécurité spécifiques à suivre dans le cadre de leurs fonctions pour en garantir l'efficacité.</p> <p>Les formations peuvent être organisées en interne ou prodiguées par des parties tierces, notamment SANS ou PCI SSC (PCI Awareness, PCIP et ISA), des marques de paiement et des acquéreurs. Le contenu des formations doit s'appliquer à une fonction donnée et couvrir les dernières menaces de sécurité et/ou la dernière version de la norme PCI DSS.</p> <p>Pour obtenir des directives supplémentaires sur l'élaboration du contenu de formation sur la sécurité destiné aux rôles spécialisés, se reporter aux informations complémentaires sur PCI SSC - <i>Meilleures pratiques pour implémenter un programme de sensibilisation à la sécurité.</i></p>
<p>A3.2 Documenter et valider le champ d'application de la norme PCI DSS</p>		
<p>A3.2.1 Documenter et confirmer l'exactitude du champ d'application de la norme PCI DSS au moins une fois par trimestre et suite à des modifications importantes apportées à l'environnement concerné. Une validation de ce champ d'application doit être prévue au</p>	<p>A3.2.1.a Examiner les résultats documentés des examens concernés et interroger le personnel pour vérifier que les examens ont lieu :</p> <ul style="list-style-type: none"> • Au moins une fois par trimestre • Après des modifications importantes apportées à l'environnement concerné 	<p>Le champ d'application de la norme PCI DSS doit être validé aussi fréquemment que possible pour en assurer la tenue à jour et la mise en correspondance avec les objectifs commerciaux en constante évolution</p>

Conditions A3	Procédures de test	Directive
<p>moins une fois par trimestre et comprendre ce qui suit :</p> <ul style="list-style-type: none"> • Identification de tous les réseaux concernés et composants de système • Identification de tous les réseaux hors champ d'application et justification des réseaux hors champ d'application, y compris les descriptions de tous les contrôles de segmentation implémentés • Identification de toutes les entités connectées, notamment les entités tierces avec un droit d'accès à l'environnement des données de titulaires de carte (CDE). <p>Référence de la norme PCI DSS : <i>Champ d'application des conditions de la norme PCI DSS</i></p>	<p>A3.2.1.b Examiner les résultats documentés des examens trimestriels pour vérifier ce qui suit :</p> <ul style="list-style-type: none"> • Identification de tous les réseaux concernés et composants de système • Identification de tous les réseaux hors champ d'application et justification des réseaux étant hors champ d'application, y compris les descriptions de tous les contrôles de segmentation implémentés • Identification de toutes les entités connectées, notamment les entités tierces avec un droit d'accès à l'environnement des données de titulaires de carte (CDE) 	

Conditions A3	Procédures de test	Directive
<p>A3.2.2 Déterminer l'impact sur le champ d'application de la norme PCI DSS pour toutes les modifications apportées au système ou aux réseaux, y compris les ajouts de nouveaux systèmes et de nouvelles connexions au réseau. Les processus englobent ce qui suit :</p> <ul style="list-style-type: none"> • Évaluation formelle des impacts sur la norme PCI DSS • Identification des conditions de la norme PCI DSS applicables au système ou au réseau • Mise à jour du champ d'application de la norme PCI DSS, le cas échéant • Validation des résultats suite à l'évaluation des impacts par le personnel responsable (comme défini dans A3.1.3) <p>Référence de la norme PCI DSS : <i>Champ d'application des conditions de la norme PCI DSS, conditions 1-12</i></p>	<p>A3.2.2 Examiner la documentation sur les modifications et interroger le personnel pour s'assurer que pour chaque modification apportée aux systèmes ou aux réseaux :</p> <ul style="list-style-type: none"> • Les impacts sur la norme PCI DSS ont été formellement évalués. • Les conditions de la norme PCI DSS applicables aux modifications apportées au système ou au réseau ont été identifiées. • Le champ d'application de la norme PCI DSS a été mis à jour conformément à la modification. • La validation par le personnel responsable (comme défini dans A3.1.3) a été obtenue et documentée. 	<p>Des modifications apportées aux systèmes ou aux réseaux peuvent avoir un impact majeur sur le champ d'application de la norme PCI DSS. Ainsi, les changements des règles liées aux pare-feu peuvent inclure des segments réseau entiers dans le champ d'application ou de nouveaux systèmes peuvent être ajoutés au CDE qui doit être convenablement protégé.</p> <p>Envisager des processus visant à déterminer l'impact éventuel des changements apportés aux systèmes et aux réseaux sur le champ d'application de la norme PCI DSS dans l'entité dans le cadre d'un programme dédié de conformité à la norme PCI DSS ou d'un programme global de conformité et/ou de gouvernance dans l'entité.</p>

Conditions A3	Procédures de test	Directive
<p>A3.2.2.1 Suite à un changement, toutes les conditions pertinentes PCI DSS doivent être vérifiées sur tous les systèmes et réseaux, qu'ils soient nouveaux ou modifiés, et la documentation doit être mise à jour, le cas échéant. Voici des exemples, sans s'y limiter, des conditions PCI DSS à vérifier :</p> <ul style="list-style-type: none"> ▪ Le schéma du réseau est mis à jour pour illustrer les changements. ▪ Les systèmes sont configurés conformément aux normes de configuration ; tous les mots de passe par défaut sont modifiés et les services superflus sont désactivés. ▪ Les systèmes sont protégés par des contrôles obligatoires, comme le contrôle de l'intégrité des fichiers (FIM), le programme antivirus, les correctifs et la journalisation d'audit. ▪ S'assurer que les données d'identification sensibles (SAD) ne sont pas stockées et que le stockage de toutes les données de titulaires de carte est documenté et incorporé à la politique et aux procédures relatives à la conservation de données. ▪ Les nouveaux systèmes sont inclus dans le processus d'analyse trimestrielle des vulnérabilités. <p>Référence de la norme PCI DSS : <i>Champ d'application des conditions de la norme PCI DSS, condition 1-12</i></p>	<p>A3.2.2.1 Pour un échantillon de changements aux systèmes et aux réseaux, examiner les registres de changements, interroger le personnel et observer les systèmes/réseaux concernés pour s'assurer que les conditions applicables de la norme PCI DSS ont été effectivement implémentées et que la documentation a bien été mise à jour dans le cadre de ces changements.</p>	<p>Il est essentiel d'avoir des processus en place pour analyser tous les changements apportés et s'assurer que tous les contrôles appropriés de la norme PCI DSS sont effectivement appliqués aux systèmes ou aux réseaux ajoutés dans l'environnement concerné.</p> <p>L'insertion de cette validation dans les processus de gestion des changements vous permet de garantir que les inventaires de dispositifs et les normes de configuration sont mis à jour et que les contrôles de sécurité sont appliqués en fonction des besoins.</p> <p>Un processus de gestion des changements doit contenir des éléments justificatifs pour illustrer la mise en œuvre ou la conservation des conditions de la norme PCI DSS par le biais d'un processus itératif.</p>

Conditions A3	Procédures de test	Directive
<p>A3.2.3 Les changements de la structure organisationnelle (par exemple, l'intégration ou l'acquisition d'une société, le changement ou la réaffectation du personnel chargé des contrôles de sécurité) se soldent par un examen formel (interne) de l'impact sur le champ d'application de la norme PCI DSS et l'applicabilité des contrôles.</p> <p>Référence de la norme PCI DSS : <i>Condition 12</i></p>	<p>A3.2.3 Examiner les politiques et les procédures pour vérifier qu'un changement à la structure organisationnelle se solde par un examen formel de l'impact sur le champ d'application de la norme PCI DSS et l'applicabilité des contrôles.</p>	<p>La structure et la gestion d'une organisation définissent les conditions et le protocole pour assurer des opérations efficaces et sécurisées. Des modifications à cette structure pourraient avoir des effets défavorables sur les contrôles et les environnements existants en réaffectant ou en supprimant les ressources auparavant prises en charge par les contrôles PCI DSS ou en héritant des nouvelles responsabilités qui sont encore dépourvues de contrôles. C'est pourquoi, il est important de réexaminer le champ d'application et les contrôles de la norme PCI DSS en cas de modifications pour s'assurer que ces contrôles sont en place et actifs.</p>
<p>A3.2.4 En cas de segmentation, confirmer le champ d'application de la norme PCI DSS en effectuant des tests de pénétration sur les contrôles de segmentation au moins une fois par semestre et après des changements apportés aux contrôles/méthodes de segmentation.</p> <p>Référence de la norme PCI DSS : <i>Condition 11</i></p>	<p>A3.2.4 Examiner les résultats du dernier test de pénétration pour vérifier ce qui suit :</p> <ul style="list-style-type: none"> • Le test de pénétration est effectué pour vérifier les contrôles de segmentation au moins une fois par semestre et après des modifications apportées aux contrôles/méthodes de segmentation. • Le test de pénétration couvre tous les contrôles/toutes les méthodes de segmentation utilisées. • Le test de pénétration vérifie que les contrôles/méthodes de segmentation sont opérationnel(le)s et efficaces, et isole tous les systèmes hors de portée des systèmes dans le CDE. 	<p>Si la segmentation sert à isoler les réseaux concernés des réseaux hors champ d'application, ces contrôles de segmentation doivent être vérifiés par le biais du test de pénétration pour confirmer leur fonctionnement prévu et efficace. Les techniques des tests de pénétration doivent respecter la méthodologie de pénétration existante, comme spécifié dans la condition 11 relative à la norme PCI DSS.</p> <p>Pour obtenir des informations supplémentaires sur un test de pénétration efficace, se reporter aux Informations complémentaires sur la norme PCI SSC dans les <i>Consignes du test de pénétration</i>.</p>

Conditions A3	Procédures de test	Directive
<p>A3.2.5 Implémenter une méthodologie d'exploration des données pour confirmer le champ d'application de la norme PCI DSS et pour localiser toutes les sources et tous les emplacements du PAN en texte clair au moins une fois par trimestre et lors de modifications importantes apportées à l'environnement ou aux processus du titulaire de carte.</p> <p>La méthodologie d'exploration des données doit tenir compte du fait que du PAN en texte clair puisse résider sur des systèmes et des réseaux en dehors du CDE actuellement défini.</p> <p>Référence de la norme PCI DSS : <i>Champ d'application des conditions de la norme PCI DSS</i></p>	<p>A3.2.5.a Examiner la méthodologie d'exploration des données documentée pour vérifier ce qui suit :</p> <ul style="list-style-type: none"> • La méthodologie d'exploration des données inclut les processus destinés à identifier toutes les sources et tous les emplacements du PAN en texte clair. • Cette méthodologie tient compte du fait que du PAN en texte clair puisse résider sur des systèmes et des réseaux en dehors du CDE actuellement défini. <p>A3.2.5.b Examiner les résultats suite à une exploration récente des données et interroger le personnel pour vérifier que cette exploration a lieu au moins une fois par trimestre et lors de modifications importantes apportées à l'environnement ou aux processus du titulaire de carte.</p>	<p>Lors de la détermination du champ d'application, la norme PCI DSS exige que les entités évaluées identifient et documentent l'existence de tous les PAN en texte clair dans leurs environnements. L'implémentation d'une méthodologie d'exploration des données, qui identifie toutes les sources et tous les emplacements du PAN en texte clair et tient compte du fait que du PAN en texte clair puisse résider sur des systèmes et des réseaux en dehors du CDE actuellement défini ou à des endroits non prévus dans le CDE défini, comme un journal d'erreurs ou un fichier de vidage de la mémoire, permet de garantir que les emplacements précédemment inconnus du PAN en texte clair sont désormais détectés et sécurisés correctement.</p> <p>Les données peuvent être explorées de plusieurs manières, y compris, mais sans s'y limiter, en utilisant : (1) un logiciel d'exploration des données disponible dans le commerce, (2) un programme d'exploration des données conçu en interne ou (3) une recherche manuelle. Quelle que soit la méthode utilisée, il s'agit de trouver toutes les sources et tous les emplacements du PAN en texte clair (et pas seulement dans le CDE défini).</p>
<p>A3.2.5.1 Assurer l'efficacité des méthodes destinées à l'exploration des données. En effet, ces méthodes doivent pouvoir identifier le PAN en texte clair sur tous les types de composants de système (par exemple dans chaque système d'exploitation ou plateforme) et les formats de fichiers utilisés.</p> <p>L'efficacité des méthodes d'exploration des</p>	<p>A3.2.5.1.a Interroger le personnel et consulter la documentation pour vérifier ce qui suit :</p> <ul style="list-style-type: none"> ▪ L'entité dispose d'un processus pour tester l'efficacité des méthodes utilisées dans l'exploration des données. ▪ Ce processus doit vérifier que les méthodes en place sont capables d'identifier le PAN en texte clair sur tous les types de composants de système et les formats de fichiers utilisés. 	<p>Un processus conçu pour tester l'efficacité des méthodes d'exploration des données garantit la détection des données de titulaires de carte en toute exhaustivité et précision. Dans un souci d'exhaustivité, vous devez inclure au moins un échantillonnage de composants de système autant pour les réseaux concernés que pour les réseaux hors champ d'application dans l'exploration des données. Pour tester la</p>

Conditions A3	Procédures de test	Directive
<p>données doit être confirmée au moins une fois par an.</p> <p>Référence de la norme PCI DSS : Champ d'application des conditions de la norme PCI DSS</p>	<p>A3.2.5.1.b Examiner les résultats des tests récents d'efficacité pour vérifier que la fiabilité des méthodes destinées à l'exploration des données est effectivement confirmée une fois par an.</p>	<p>précision, insérez des PAN dans un échantillon de composants de système et de formats de fichiers utilisés et confirmez que l'exploration des données a effectivement détecté ces PAN.</p>
<p>A3.2.5.2 Implémenter les procédures suivantes d'intervention à lancer lorsque le PAN en texte clair est détecté en dehors du CDE :</p> <ul style="list-style-type: none"> ▪ Procédures pour déterminer la marche à suivre si un PAN en texte clair est identifié en dehors du CDE, y compris son retrait, sa suppression sécurisée et/ou sa migration vers le CDE actuellement défini, le cas échéant ▪ Procédures pour expliquer comment les données ont quitté le CDE ▪ Procédures pour résoudre les fuites de données ou les failles des processus, qui se sont soldées par la sortie des données du CDE ▪ Procédures pour identifier la source des données ▪ Procédures pour identifier si des données de piste sont stockées avec les PAN 	<p>A3.2.5.2.a Examiner les procédures d'intervention documentées pour vérifier qu'elles sont définies convenablement si le PAN en texte clair est détecté en dehors du CDE, et qu'elles comprennent ce qui suit :</p> <ul style="list-style-type: none"> ▪ Procédures pour déterminer la marche à suivre si un PAN en texte clair est identifié en dehors du CDE, y compris son retrait, sa suppression sécurisée et/ou sa migration vers le CDE actuellement défini, le cas échéant ▪ Procédures pour expliquer comment les données ont quitté le CDE ▪ Procédures pour résoudre les fuites de données ou les failles des processus, qui se sont soldées par la sortie des données du CDE ▪ Procédures pour identifier la source des données ▪ Procédures pour identifier si des données de piste sont stockées avec les PAN <p>A3.2.5.2.b Interroger le personnel et examiner les mesures correctives pour s'assurer que des activités de résolution sont effectuées lorsque le PAN en texte clair est détecté en dehors du CDE.</p>	<p>Des procédures d'interventions documentées, à suivre si le PAN en texte clair est détecté en dehors du CDE, permettent d'identifier les mesures correctives et de prévenir des fuites à venir. Par exemple, si le PAN a été localisé en dehors du CDE, procéder à une analyse pour (1) déterminer s'il a été enregistré indépendamment des autres données (ou s'il faisait partie de données de piste complètes), (2) identifier la source des données et (3) identifier les failles de contrôle qui se sont soldées par la sortie des données du CDE.</p>

Conditions A3	Procédures de test	Directive
<p>A3.2.6 Implémenter les mécanismes requis pour détecter le PAN en texte clair et l'empêcher de quitter le CDE via un canal non autorisé, une méthode ou un processus illicite, y compris la création de journaux d'audit et d'alertes.</p> <p>Référence de la norme PCI DSS : <i>Champ d'application des conditions de la norme PCI DSS</i></p>	<p>A3.2.6.a Examiner la documentation et observer les mesures en place pour vérifier que les mécanismes :</p> <ul style="list-style-type: none"> • Sont implémentés et fonctionnent activement • Sont configurés pour détecter le PAN en texte clair et l'empêcher de quitter le CDE via un canal non autorisé, une méthode ou un processus illicite • Génèrent des journaux et des alertes si le PAN en texte clair quitte le CDE via un canal non autorisé, une méthode ou un processus illicite <p>A3.2.6.b Examiner les journaux d'audit et les alertes, et interroger le personnel responsable pour s'assurer que les alertes font l'objet d'une enquête.</p>	<p>Les mécanismes prévus pour détecter et pour empêcher la perte non autorisée du PAN en texte clair peuvent comprendre des outils adaptés, comme les solutions de prévention de la perte de données (data loss prevention, DLP), et/ou des processus et procédures manuels. Parmi ces mécanismes, on peut compter, mais sans s'y limiter, les e-mails, les téléchargements sur des supports amovibles et les sorties pour imprimantes. Grâce à ces mécanismes, une organisation peut détecter et prévenir des situations susceptibles de se solder par une perte de données.</p>
<p>A3.2.6.1 Implémenter les procédures d'intervention à lancer en cas de tentative de suppression du PAN en texte clair du CDE via un canal non autorisé, une méthode ou un processus illicite. Les procédures d'intervention incluent ce qui suit :</p> <ul style="list-style-type: none"> ▪ Procédures destinées au personnel chargé de mener des enquêtes opportunes suite à des alertes ▪ Procédures pour résoudre les fuites de données ou les failles des processus, le cas échéant, pour empêcher toute perte de données 	<p>A3.2.6.1.a Examiner les procédures d'intervention documentées pour vérifier qu'elles sont lancées en cas de tentative de suppression du PAN en texte clair du CDE via un canal non autorisé, une méthode ou un processus illicite, et qu'elles comprennent ce qui suit :</p> <ul style="list-style-type: none"> ▪ Procédures destinées au personnel chargé de mener des enquêtes opportunes suite à des alertes ▪ Procédures pour résoudre les fuites de données ou les failles des processus, le cas échéant, pour empêcher toute perte de données <p>A3.2.6.1.b Interroger le personnel et examiner les mesures prises lorsque le PAN en texte clair est détecté en dehors du CDE via un canal non autorisé, une méthode ou un processus illicite, et s'assurer que des activités de résolution sont effectuées.</p>	<p>Des tentatives de suppression du PAN en texte clair du CDE via un canal non autorisé, une méthode ou un processus illicite peuvent signaler une intention malveillante de voler des données ou peuvent résulter des actes d'un employé autorisé qui n'en est pas conscient ou qui ne suit tout simplement pas les consignes adéquates. Une enquête opportune de ces incidents peut orienter les besoins de résolution et fournir des informations précieuses pour mieux comprendre la source des menaces.</p>
<p>A3.3 Confirmer que la norme PCI DSS est incorporée dans les activités courantes (BAU)</p>		
<p>A3.3.1 Implémenter un processus pour détecter et signaler immédiatement des pannes de contrôle de sécurité critique.</p>	<p>A3.3.1.a Examiner les politiques et les procédures documentées pour vérifier que les processus sont définis pour détecter et signaler immédiatement des</p>	<p>À défaut de processus formels pour détecter et signaler rapidement (dès que possible) les pannes de contrôles de sécurité critiques, les</p>

Conditions A3	Procédures de test	Directive
<p>Exemples de contrôle de sécurité critique (non exhaustifs) :</p> <ul style="list-style-type: none"> • Pare-feu • IDS/IPS • FIM • Antivirus • Contrôles d'accès physiques • Contrôles d'accès logiques • Mécanismes de journalisation d'audit • Contrôles de segmentation (le cas échéant) <p>Référence de la norme PCI DSS : Conditions 1-12</p>	<p>pannes de contrôles de sécurité critiques.</p> <p>A3.3.1.b Examiner les processus de détection et d'alerte et interroger le personnel pour vérifier que les processus sont implémentés pour tous les contrôles de sécurité critiques et que la panne d'un tel contrôle se solde par le déclenchement d'une alerte.</p>	<p>pannes peuvent ne pas être détectées pendant des périodes prolongées et peuvent procurer aux pirates tout le temps nécessaire pour compromettre les systèmes et pour voler des données confidentielles dans l'environnement des données de titulaires de carte.</p>

Conditions A3	Procédures de test	Directive
<p>A3.3.1.1 Intervenir face aux pannes de contrôles de sécurité critiques en temps opportun. Les processus de résolution des pannes de contrôles de sécurité doivent comprendre :</p> <ul style="list-style-type: none"> ▪ Rétablissement des fonctions de sécurité ▪ Identification et documentation de la durée (date et heure de début et de fin) de la panne de sécurité ▪ Identification et documentation des causes de la panne, y compris la cause fondamentale, et documentation des rectificatifs requis pour résoudre la cause fondamentale ▪ Identification et résolution des problèmes de sécurité survenus pendant la panne ▪ Évaluation des risques pour déterminer si d'autres actions sont indispensables suite à une panne de sécurité ▪ Implémentation des contrôles pour prévenir la répétition d'une telle panne ▪ Reprise de la surveillance des contrôles de sécurité <p>Référence de la norme PCI DSS : Conditions 1-12</p>	<p>A3.3.1.1.a Examiner les politiques et les procédures documentées et interroger le personnel pour vérifier que les processus sont définis et implémentés pour résoudre une panne de contrôle de sécurité et qu'ils comprennent :</p> <ul style="list-style-type: none"> ▪ Rétablissement des fonctions de sécurité ▪ Identification et documentation de la durée (date et heure de début et de fin) de la panne de sécurité ▪ Identification et documentation des causes de la panne, y compris la cause fondamentale, et documentation des rectificatifs requis pour résoudre la cause fondamentale ▪ Identification et résolution des problèmes de sécurité survenus pendant la panne ▪ Évaluation des risques pour déterminer si d'autres actions sont indispensables suite à une panne de sécurité ▪ Implémentation des contrôles pour prévenir la répétition d'une telle panne ▪ Reprise de la surveillance des contrôles de sécurité <p>A3.3.1.1.b Examiner les registres pour vérifier que les pannes des contrôles de sécurité sont documentées et comprennent ce qui suit :</p> <ul style="list-style-type: none"> ▪ Identification des causes de la panne, y compris la cause fondamentale ▪ Durée (date et heure de début et de fin) de la panne de sécurité ▪ Détails de la résolution requise pour rectifier la cause fondamentale 	<p>Les justificatifs documentés (par exemple, des registres dans un système de gestion des problèmes) doivent indiquer que des processus et des procédures sont implémentés pour résoudre les pannes de sécurité. Qui plus est, le personnel doit être conscient de ses responsabilités en cas de panne. Les mesures et les interventions relatives aux pannes doivent être présentées dans les justificatifs documentés.</p>

Conditions A3	Procédures de test	Directive
<p>A3.3.2 Examiner les technologies matérielles et logicielles au moins une fois par an pour confirmer qu'elles continuent de respecter les conditions de la norme PCI DSS au sein de l'organisation. (Par exemple, un examen des technologies qui ne sont plus prises en charge par le fournisseur et/ou qui ne répondent plus aux besoins de sécurité de l'organisation.)</p> <p>Ce processus suppose un plan pour gérer les technologies qui ne remplissent plus les conditions de la norme PCI DSS dans l'organisation. Ce plan peut inclure, mais sans s'y limiter, le remplacement des technologies, le cas échéant.</p> <p>Référence de la norme PCI DSS : Conditions 2, 6</p>	<p>A3.3.2.a Examiner les politiques et les procédures documentées et interroger le personnel pour vérifier que les processus sont définis et implémentés pour contrôler les technologies matérielles et logicielles et confirmer qu'elles continuent de satisfaire les conditions de la norme PCI DSS au sein de l'organisation.</p> <p>A3.3.2.b Examiner les résultats récents pour vérifier que les contrôles ont lieu au moins une fois par an.</p> <p>A3.3.2.c Vérifier le plan en vigueur pour remplacer les technologies ne satisfaisant plus les conditions de la norme de PCI DSS au sein de l'organisation.</p>	<p>Les technologies matérielles et logicielles sont en constante évolution. Les organisations doivent être conscientes des modifications apportées aux technologies qu'elles utilisent et des menaces qui pèsent sur elles. Les organisations doivent également se tenir informées des modifications initiées par les prestataires technologiques sur leurs produits ou leurs processus d'assistance. Ainsi, elles pourront mieux appréhender ces changements et leur impact sur les technologies exploitées.</p> <p>Des examens fréquents des technologies susceptibles d'avoir un impact sur les contrôles de la norme PCI DSS, ou de les influencer, peuvent contribuer aux stratégies en matière d'achat, d'utilisation et de déploiement, et assurer l'efficacité ininterrompue des contrôles dépendant de ces technologies.</p>

Conditions A3	Procédures de test	Directive
<p>A3.3.3 Procéder aux examens au moins une fois par trimestre pour vérifier que les activités BAU sont conformes. Il incombe au personnel chargé de l'implémentation du programme de conformité à la norme PCI DSS d'effectuer ces examens (comme stipulé dans la condition A3.1.3) et de procéder comme suit :</p> <ul style="list-style-type: none"> • Confirmer que toutes les activités BAU (A3.2.2, A3.2.6 et A3.3.1) sont exécutées • Confirmer que le personnel respecte les politiques de sécurité et les procédures opérationnelles (par exemple, les examens quotidiens des journaux, les examens des règles liées aux pare-feu, les normes de configuration pour les nouveaux systèmes, etc.) • Documenter l'exécution des examens, y compris le mode de vérification de toutes les activités BAU en place • Rassembler les justificatifs documentés conformément aux exigences d'évaluation annuelle de la norme PCI DSS • Examiner et valider les résultats par le personnel responsable du programme de conformité à la norme PCI DSS (comme stipulé dans la condition A3.1.3) • Conserver les registres et la documentation pendant au moins 12 mois, y compris toutes les activités BAU <p>Référence de la norme PCI DSS :</p>	<p>A3.3.3.a Examiner les politiques et les procédures pour vérifier que les processus sont définis pour l'examen et le contrôle des activités BAU. Vérifier que les procédures comprennent ce qui suit :</p> <ul style="list-style-type: none"> • Confirmer que toutes les activités BAU (A3.2.2, A3.2.6 et A3.3.1) sont exécutées • Confirmer que le personnel respecte les politiques de sécurité et les procédures opérationnelles (par exemple, les examens quotidiens des journaux, les examens des règles liées aux pare-feu, les normes de configuration pour les nouveaux systèmes, etc.) • Documenter l'exécution des examens, y compris le mode de vérification de toutes les activités BAU en place • Rassembler les justificatifs documentés conformément aux exigences d'évaluation annuelle de la norme PCI DSS • Examiner et valider les résultats par l'équipe de direction chargée de la gouvernance de la norme PCI DSS • Conserver les registres et la documentation pendant au moins 12 mois, y compris toutes les activités BAU <p>A3.3.3.b Interroger le personnel responsable et examiner les registres des examens pour vérifier que :</p> <ul style="list-style-type: none"> • Les examens sont menés par le personnel chargé de l'implémentation du programme de conformité à la norme PCI DSS • Les examens sont effectués au moins une fois par trimestre 	<p>Mettre en œuvre les contrôles de la norme PCI DSS dans les processus d'affaires courantes fait partie des opérations commerciales normales et régulières. C'est pourquoi il est important que des contrôles indépendants soient menés pour garantir que les contrôles BAU sont actifs et fonctionnent comme prévu.</p> <p>Ces contrôles indépendants visent à examiner les justificatifs qui confirment l'exécution d'activités courantes.</p> <p>Ces examens peuvent également être utilisés pour vérifier que des preuves suffisantes sont maintenues, par exemple, des journaux d'audit, des rapports d'analyse de vulnérabilité, des examens de pare-feu, etc. afin d'aider l'entité à se préparer pour sa prochaine évaluation de conformité à la norme PCI DSS.</p>

Conditions A3	Procédures de test	Directive
<i>Conditions 1-12</i>		
A3.4 Contrôler et gérer l'accès logique à l'environnement des données de titulaires de carte		
<p>A3.4.1 Examiner les comptes d'utilisateur et les privilèges d'accès aux composants de système concernés au moins une fois par semestre pour confirmer qu'ils sont encore adaptés à la fonction et autorisés comme il se doit.</p> <p>Référence de la norme PCI DSS : <i>Condition 7</i></p>	<p>A3.4.1 Interroger le personnel responsable et examiner la documentation connexe pour vérifier que :</p> <ul style="list-style-type: none"> • Les comptes d'utilisateur et les privilèges d'accès sont examinés une fois par semestre. • Les examens confirment que les privilèges d'accès sont adaptés à la fonction et autorisés comme il se doit. 	<p>Les exigences relatives aux privilèges d'accès évoluent avec le temps dans la mesure où les individus changent de poste ou quittent la société, et leurs fonctions exercées évoluent. L'équipe de direction est tenue d'examiner, de valider et de mettre à jour les droits d'accès des utilisateurs régulièrement et en fonction des besoins pour refléter les changements dans le personnel, y compris les parties tierces, et dans les fonctions exercées par les utilisateurs.</p>
A3.5 Identifier et résoudre les événements suspects		
<p>A3.5.1 Implémenter une méthodologie pour identifier rapidement les modèles d'attaques et le comportement indésirable sur les systèmes, par exemple en effectuant des examens manuels coordonnés et/ou en utilisant des outils de corrélation de journaux automatisés ou avec une gestion centralisée, pour inclure au minimum ce qui suit :</p> <ul style="list-style-type: none"> • Identification des anomalies ou des activités suspectes en temps réel • Déclenchement d'alertes opportunes lorsque le personnel détecte des activités suspectes ou des anomalies • Intervention face aux alertes conformément aux procédures d'intervention documentées <p>Référence de la norme PCI DSS : <i>Conditions 10, 12</i></p>	<p>A3.5.1.a Examiner la documentation et interroger le personnel pour vérifier qu'une méthodologie est définie et mise en œuvre pour identifier rapidement les modèles d'attaques et le comportement indésirable sur les systèmes, comme suit :</p> <ul style="list-style-type: none"> • Identification des anomalies ou des activités suspectes en temps réel • Déclenchement d'alertes opportunes au personnel responsable • Intervention face aux alertes conformément aux procédures d'intervention documentées <p>A3.5.1.b Examiner les procédures de réponse aux incidents et interroger le personnel pour vérifier que :</p> <ul style="list-style-type: none"> • Le personnel de garde reçoit des alertes en temps opportun. • Les alertes sont traitées conformément aux procédures d'intervention documentées. 	<p>Identifier les modèles d'attaques et le comportement indésirable sur les systèmes est essentiel pour empêcher, détecter ou minimiser l'impact d'un incident de sécurité sur les données. La présence de journaux dans tous les environnements permet de suivre de près, d'émettre des alertes et d'analyser les incidents éventuels. Déterminer la cause d'un incident de sécurité est très délicat, voire impossible, sans corroborer les informations entre les composants de systèmes critiques et les systèmes chargés des fonctions de sécurité, comme les pare-feu, IDS/IP et les contrôles de l'intégrité des fichiers (FIM). C'est pourquoi il est essentiel de rassembler, corréler et gérer les journaux pour tous les composants de système critiques et les systèmes chargés des fonctions de sécurité. Cette mesure peut comprendre le recours à des produits logiciels et des méthodologies de services pour garantir une analyse en temps réel, des alertes et des</p>

Conditions A3	Procédures de test	Directive
		créations de rapports, comme la gestion d'informations et d'événements de sécurité (GIES), le contrôle de l'intégrité des fichiers (FIM) ou la détection des modifications.

Annexe B : Contrôles compensatoires

Des contrôles compensatoires peuvent être envisagés lorsqu'une entité ne peut pas se conformer aux conditions de la norme PCI DSS comme stipulées, en raison de contraintes commerciales documentées ou de contraintes techniques légitimes, mais qu'elle a parallèlement suffisamment atténué les risques associés par la mise en œuvre d'autres contrôles, appelés « contrôles compensatoires ».

Les contrôles compensatoires doivent satisfaire aux critères suivants :

1. Respecter l'intention et la rigueur de la condition initiale de la norme PCI DSS.
2. Fournir une protection similaire à celle de la condition initiale de la norme PCI DSS, de sorte que le contrôle compensatoire compense suffisamment le risque prévenu par la condition initiale. (Pour plus d'informations sur chaque condition PCI DSS, voir *Navigation dans la norme PCI DSS*.)
3. Aller au-delà des autres conditions PCI DSS (Les contrôles compensatoires ne consistent pas simplement en la conformité à d'autres conditions PCI DSS.)

Lors de l'évaluation de la portée des contrôles compensatoires, considérer les points suivants :

Remarque : les points a) à c) ci-dessous sont cités à titre d'exemple seulement. L'évaluateur qui effectue l'examen de la norme PCI DSS doit déterminer et valider la suffisance de tous les contrôles compensatoires. L'efficacité d'un contrôle compensatoire dépend des caractéristiques spécifiques de l'environnement dans lequel il est déployé, des contrôles de sécurité associés et de la configuration du contrôle proprement dit. Les sociétés doivent avoir conscience qu'un contrôle compensatoire particulier ne sera pas efficace dans tous les environnements.

- a) Les conditions existantes de la norme PCI DSS NE PEUVENT PAS être considérées comme des contrôles compensatoires si elles sont déjà exigées pour l'élément examiné. Par exemple, les mots de passe pour l'accès administrateur non-console doivent être transmis sous forme cryptée afin de restreindre les risques d'interception des mots de passe administrateur en texte clair. Une entité ne peut pas utiliser d'autres conditions de mot de passe de la norme PCI DSS (blocage des intrus, mots de passe complexes, etc.) pour compenser l'absence de mots de passe cryptés, puisque celles-ci ne limitent pas les risques d'interception des mots de passe en texte clair. Par ailleurs, les autres contrôles de mots de passe sont déjà exigés par la norme PCI DSS pour l'élément examiné (à savoir les mots de passe).
 - b) Les conditions existantes de la norme PCI DSS PEUVENT être considérées comme des contrôles compensatoires si elles sont exigées dans un autre domaine, mais pas pour l'élément examiné. Par exemple, l'authentification à plusieurs facteurs est exigée par la norme PCI DSS pour l'accès à distance. L'authentification à plusieurs facteurs *à partir du réseau interne* peut aussi être considérée comme un contrôle compensatoire de l'accès administrateur non-console lorsque la transmission des mots de passe cryptés ne peut pas être prise en charge. L'authentification à plusieurs facteurs est un contrôle compensatoire acceptable si : (1) elle satisfait à l'intention de la condition initiale en résolvant les risques d'interception des mots de passe administrateur en texte clair, et (2) elle est correctement configurée et mise en œuvre dans un environnement sécurisé.
 - c) Les conditions existantes de la norme PCI DSS peuvent être associées à de nouveaux contrôles et constituer alors un contrôle compensatoire. Par exemple, si une société n'est pas en mesure de rendre les données de titulaires de carte illisibles conformément à la condition 3.4 (par exemple, par cryptage), un contrôle compensatoire pourrait consister en un dispositif ou un ensemble de dispositifs, d'applications et de contrôles qui assurent : (1) la segmentation du réseau interne ; (2) le filtrage des adresses IP ou MAC ; et (3) l'authentification à plusieurs facteurs à partir du réseau interne.
4. Être proportionnels aux risques supplémentaires qu'implique le non-respect de la condition PCI DSS.

L'évaluateur doit évaluer soigneusement les contrôles compensatoires pendant chaque évaluation annuelle de la norme PCI DSS afin de confirmer que chaque contrôle compensatoire couvre de manière appropriée le risque ciblé par la condition initiale de la norme PCI DSS, conformément aux points 1 à 4 présentés ci-dessus. Pour maintenir la conformité, des processus et des contrôles doivent être en place pour garantir que les contrôles compensatoires restent efficaces après l'évaluation.

Annexe C : Fiche de contrôles compensatoires

Se référer à cette fiche pour définir les contrôles compensatoires dans toute situation où ces contrôles sont utilisés pour satisfaire une condition PCI DSS. Noter que les contrôles compensatoires doivent être documentés dans le Rapport sur la conformité, dans la section de la clause PCI DSS correspondante.

Remarque : *Seules les entreprises qui ont procédé à une analyse des risques et ont des contraintes commerciales documentées ou des contraintes technologiques légitimes peuvent envisager l'utilisation de contrôles compensatoires pour se mettre en conformité.*

Numéro et définition des clauses :

	Informations requises	Explication
1. Contraintes	Répertorier les contraintes qui empêchent la conformité à la condition initiale.	
2. Objectif	Définir l'objectif du contrôle initial ; identifier l'objectif satisfait par le contrôle compensatoire.	
3. Risque identifié	Identifier tous les risques supplémentaires qu'induit l'absence du contrôle initial.	
4. Définition des contrôles compensatoires	Définir les contrôles compensatoires et expliquer comment ils satisfont les objectifs du contrôle initial et résolvent les risques supplémentaires éventuels.	
5. Validation des contrôles compensatoires	Définir comment les contrôles compensatoires ont été validés et testés.	
6. Gestion	Définir les processus et les contrôles en place pour la gestion des contrôles compensatoires.	

Fiche de contrôles compensatoires – Exemple complété

Utiliser cette fiche de travail pour définir les contrôles compensatoires pour toute condition reconnue « en place » par le biais de ces contrôles.

Numéro de clause : 8.1.1 – *Tous les utilisateurs sont-ils identifiés avec un ID utilisateur unique leur permettant d'accéder aux composants de système et aux données de titulaires de carte ?*

	Informations requises	Explication
1. Contraintes	Répertorier les contraintes qui empêchent la conformité à la condition initiale.	<i>La société XYZ utilise des serveurs Unix autonomes sans LDAP. Par conséquent, chacun requiert un nom d'utilisateur « racine ». La société XYZ ne peut pas gérer le nom d'utilisateur « racine » ni consigner toutes les activités de chaque utilisateur « racine ».</i>
2. Objectif	Définir l'objectif du contrôle initial ; identifier l'objectif satisfait par le contrôle compensatoire.	<i>L'exigence de noms d'utilisateur uniques vise un double objectif. Premièrement, le partage des informations d'identification n'est pas acceptable du point de vue de la sécurité. Deuxièmement, le partage des noms d'utilisateur rend impossible l'identification de la personne responsable d'une action particulière.</i>
3. Risque identifié	Identifier tous les risques supplémentaires qu'induit l'absence du contrôle initial.	<i>L'absence d'ID d'utilisateur unique et le fait de ne pas pouvoir tracer les informations d'identification introduisent des risques supplémentaires dans le système de contrôle d'accès.</i>
4. Définition des contrôles compensatoires	Définir les contrôles compensatoires et expliquer comment ils satisfont les objectifs du contrôle initial et résolvent les risques supplémentaires éventuels.	<i>La société XYZ exige que tous ses utilisateurs se connectent aux serveurs avec leurs comptes d'utilisateurs standard, et utilisent alors la commande « sudo » pour exécuter toutes commandes administratives. C'est ainsi qu'ils pourront utiliser les privilèges de comptes « racine » pour exécuter des commandes prédéfinies enregistrées par sudo dans le journal de sécurité. De cette manière, les actions de chaque utilisateur peuvent être suivies grâce à un compte utilisateur individuel sans que le mot de passe « racine » soit partagé avec d'autres utilisateurs.</i>

5. Validation des contrôles compensatoires	Définir comment les contrôles compensatoires ont été validés et testés.	<i>La société XYZ prouve à l'évaluateur que la commande sudo est configurée correctement à l'aide d'un fichier « sudoers », que seules les commandes prédéfinies peuvent être exécutées par des utilisateurs spécifiques, et que toutes les activités de ces individus utilisant la commande sudo sont consignées afin d'identifier les actions effectuées à l'aide des privilèges « racine ».</i>
6. Gestion	Définir les processus et les contrôles en place pour la gestion des contrôles compensatoires.	<i>La société XYZ documente les processus et les procédures pour éviter la modification, l'altération ou la suppression des configurations sudo de sorte que des utilisateurs individuels puissent exécuter des commandes racine sans que leurs activités soient identifiées, suivies et consignées.</i>

Annexe D : Segmentation et échantillonnage des installations de l'entreprise et des composants de système

